

Public Administration and Public Policy/101

Science and Technology of Terrorism and Counterterrorism

edited by

Tushar K. Ghosh

Mark A. Prelas

Dabir S. Viswanath

Sudarshan K. Loyalka

Science and Technology of Terrorism and Counterterrorism

edited by

Tushar K. Ghosh

Mark A. Prelas

Dabir S. Viswanath

Sudarshan K. Loyalka

*University of Missouri
Columbia, Missouri*



MARCEL DEKKER, INC.

NEW YORK • BASEL

ISBN: 0-8247-0870-9

This book is printed on acid-free paper.

Headquarters

Marcel Dekker, Inc.
270 Madison Avenue, New York, NY 10016
tel: 212-696-9000; fax: 212-685-4540

Eastern Hemisphere Distribution

Marcel Dekker AG
Hutgasse 4, Postfach 812, CH-4001 Basel, Switzerland
tel: 41-61-260-6300; fax: 41-61-260-6333

World Wide Web

<http://www.dekker.com>

The publisher offers discounts on this book when ordered in bulk quantities. For more information, write to Special Sales/Professional Marketing at the headquarters address above.

Copyright © 2002 by Marcel Dekker, Inc. All Rights Reserved.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage and retrieval system, without permission in writing from the publisher.

Current printing (last digit):

10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

PUBLIC ADMINISTRATION AND PUBLIC POLICY

A Comprehensive Publication Program

Executive Editor

JACK RABIN

Professor of Public Administration and Public Policy
School of Public Affairs
The Capital College
The Pennsylvania State University—Harrisburg
Middletown, Pennsylvania

1. *Public Administration as a Developing Discipline* (in two parts), Robert T. Golembiewski
2. *Comparative National Policies on Health Care*, Milton I. Roemer, M.D.
3. *Exclusionary Injustice: The Problem of Illegally Obtained Evidence*, Steven R. Schlesinger
4. *Personnel Management in Government: Politics and Process*, Jay M. Shafritz, Walter L. Balk, Albert C. Hyde, and David H. Rosenbloom
5. *Organization Development in Public Administration* (in two parts), edited by Robert T. Golembiewski and William B. Eddy
6. *Public Administration: A Comparative Perspective, Second Edition, Revised and Expanded*, Ferrel Heady
7. *Approaches to Planned Change* (in two parts), Robert T. Golembiewski
8. *Program Evaluation at HEW* (in three parts), edited by James G. Abert
9. *The States and the Metropolis*, Patricia S. Florestano and Vincent L. Marando
10. *Personnel Management in Government: Politics and Process, Second Edition, Revised and Expanded*, Jay M. Shafritz, Albert C. Hyde, and David H. Rosenbloom
11. *Changing Bureaucracies: Understanding the Organization Before Selecting the Approach*, William A. Medina
12. *Handbook on Public Budgeting and Financial Management*, edited by Jack Rabin and Thomas D. Lynch
13. *Encyclopedia of Policy Studies*, edited by Stuart S. Nagel
14. *Public Administration and Law: Bench v. Bureau in the United States*, David H. Rosenbloom
15. *Handbook on Public Personnel Administration and Labor Relations*, edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
16. *Public Budgeting and Finance: Behavioral, Theoretical, and Technical Perspectives, Third Edition*, edited by Robert T. Golembiewski and Jack Rabin
17. *Organizational Behavior and Public Management*, Debra W. Stewart and G. David Garson
18. *The Politics of Terrorism: Second Edition, Revised and Expanded*, edited by Michael Stohl

19. *Handbook of Organization Management*, edited by William B. Eddy
20. *Organization Theory and Management*, edited by Thomas D. Lynch
21. *Labor Relations in the Public Sector*, Richard C. Kearney
22. *Politics and Administration: Woodrow Wilson and American Public Administration*, edited by Jack Rabin and James S. Bowman
23. *Making and Managing Policy: Formulation, Analysis, Evaluation*, edited by G. Ronald Gilbert
24. *Public Administration: A Comparative Perspective, Third Edition, Revised*, Ferrel Heady
25. *Decision Making in the Public Sector*, edited by Lloyd G. Nigro
26. *Managing Administration*, edited by Jack Rabin, Samuel Humes, and Brian S. Morgan
27. *Public Personnel Update*, edited by Michael Cohen and Robert T. Golembiewski
28. *State and Local Government Administration*, edited by Jack Rabin and Don Dodd
29. *Public Administration: A Bibliographic Guide to the Literature*, Howard E. McCurdy
30. *Personnel Management in Government: Politics and Process, Third Edition, Revised and Expanded*, Jay M. Shafritz, Albert C. Hyde, and David H. Rosenbloom
31. *Handbook of Information Resource Management*, edited by Jack Rabin and Edward M. Jackowski
32. *Public Administration in Developed Democracies: A Comparative Study*, edited by Donald C. Rowat
33. *The Politics of Terrorism: Third Edition, Revised and Expanded*, edited by Michael Stohl
34. *Handbook on Human Services Administration*, edited by Jack Rabin and Marcia B. Steinhauer
35. *Handbook of Public Administration*, edited by Jack Rabin, W. Bartley Hildreth, and Gerald J. Miller
36. *Ethics for Bureaucrats: An Essay on Law and Values, Second Edition, Revised and Expanded*, John A. Rohr
37. *The Guide to the Foundations of Public Administration*, Daniel W. Martin
38. *Handbook of Strategic Management*, edited by Jack Rabin, Gerald J. Miller, and W. Bartley Hildreth
39. *Terrorism and Emergency Management: Policy and Administration*, William L. Waugh, Jr.
40. *Organizational Behavior and Public Management: Second Edition, Revised and Expanded*, Michael L. Vasu, Debra W. Stewart, and G. David Garson
41. *Handbook of Comparative and Development Public Administration*, edited by Ali Farazmand
42. *Public Administration: A Comparative Perspective, Fourth Edition*, Ferrel Heady
43. *Government Financial Management Theory*, Gerald J. Miller
44. *Personnel Management in Government: Politics and Process, Fourth Edition, Revised and Expanded*, Jay M. Shafritz, Norma M. Riccucci, David H. Rosenbloom, and Albert C. Hyde
45. *Public Productivity Handbook*, edited by Marc Holzer
46. *Handbook of Public Budgeting*, edited by Jack Rabin

-
47. *Labor Relations in the Public Sector: Second Edition, Revised and Expanded*, Richard C. Kearney
 48. *Handbook of Organizational Consultation*, edited by Robert T. Golembiewski
 49. *Handbook of Court Administration and Management*, edited by Steven W. Hays and Cole Blease Graham, Jr.
 50. *Handbook of Comparative Public Budgeting and Financial Management*, edited by Thomas D. Lynch and Lawrence L. Martin
 51. *Handbook of Organizational Behavior*, edited by Robert T. Golembiewski
 52. *Handbook of Administrative Ethics*, edited by Terry L. Cooper
 53. *Encyclopedia of Policy Studies: Second Edition, Revised and Expanded*, edited by Stuart S. Nagel
 54. *Handbook of Regulation and Administrative Law*, edited by David H. Rosenbloom and Richard D. Schwartz
 55. *Handbook of Bureaucracy*, edited by Ali Farazmand
 56. *Handbook of Public Sector Labor Relations*, edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
 57. *Practical Public Management*, Robert T. Golembiewski
 58. *Handbook of Public Personnel Administration*, edited by Jack Rabin, Thomas Vocino, W. Bartley Hildreth, and Gerald J. Miller
 59. *Public Administration: A Comparative Perspective, Fifth Edition*, Ferrel Heady
 60. *Handbook of Debt Management*, edited by Gerald J. Miller
 61. *Public Administration and Law: Second Edition*, David H. Rosenbloom and Rosemary O'Leary
 62. *Handbook of Local Government Administration*, edited by John J. Gargan
 63. *Handbook of Administrative Communication*, edited by James L. Garnett and Alexander Kouzmin
 64. *Public Budgeting and Finance: Fourth Edition, Revised and Expanded*, edited by Robert T. Golembiewski and Jack Rabin
 65. *Handbook of Public Administration: Second Edition*, edited by Jack Rabin, W. Bartley Hildreth, and Gerald J. Miller
 66. *Handbook of Organization Theory and Management: The Philosophical Approach*, edited by Thomas D. Lynch and Todd J. Dicker
 67. *Handbook of Public Finance*, edited by Fred Thompson and Mark T. Green
 68. *Organizational Behavior and Public Management: Third Edition, Revised and Expanded*, Michael L. Vasu, Debra W. Stewart, and G. David Garson
 69. *Handbook of Economic Development*, edited by Kuotsai Tom Liou
 70. *Handbook of Health Administration and Policy*, edited by Anne Osborne Kilpatrick and James A. Johnson
 71. *Handbook of Research Methods in Public Administration*, edited by Gerald J. Miller and Marcia L. Whicker
 72. *Handbook on Taxation*, edited by W. Bartley Hildreth and James A. Richardson
 73. *Handbook of Comparative Public Administration in the Asia-Pacific Basin*, edited by Hoi-kwok Wong and Hon S. Chan
 74. *Handbook of Global Environmental Policy and Administration*, edited by Dennis L. Soden and Brent S. Steel
 75. *Handbook of State Government Administration*, edited by John J. Gargan
 76. *Handbook of Global Legal Policy*, edited by Stuart S. Nagel
 77. *Handbook of Public Information Systems*, edited by G. David Garson
 78. *Handbook of Global Economic Policy*, edited by Stuart S. Nagel

79. *Handbook of Strategic Management: Second Edition, Revised and Expanded*, edited by Jack Rabin, Gerald J. Miller, and W. Bartley Hildreth
80. *Handbook of Global International Policy*, edited by Stuart S. Nagel
81. *Handbook of Organizational Consultation: Second Edition, Revised and Expanded*, edited by Robert T. Golembiewski
82. *Handbook of Global Political Policy*, edited by Stuart S. Nagel
83. *Handbook of Global Technology Policy*, edited by Stuart S. Nagel
84. *Handbook of Criminal Justice Administration*, edited by Toni DuPont-Morales, Michael K. Hooper, and Judy H. Schmidt
85. *Labor Relations in the Public Sector: Third Edition*, edited by Richard C. Kearney
86. *Handbook of Administrative Ethics: Second Edition, Revised and Expanded*, edited by Terry L. Cooper
87. *Handbook of Organizational Behavior: Second Edition, Revised and Expanded*, edited by Robert T. Golembiewski
88. *Handbook of Global Social Policy*, edited by Stuart S. Nagel and Amy Robb
89. *Public Administration: A Comparative Perspective, Sixth Edition*, Ferrel Heady
90. *Handbook of Public Quality Management*, edited by Ronald J. Stupak and Peter M. Leitner
91. *Handbook of Public Management Practice and Reform*, edited by Kuotsai Tom Liou
92. *Personnel Management in Government: Politics and Process, Fifth Edition*, Jay M. Shafritz, Norma M. Riccucci, David H. Rosenbloom, Katherine C. Naff, and Albert C. Hyde
93. *Handbook of Crisis and Emergency Management*, edited by Ali Farazmand
94. *Handbook of Comparative and Development Public Administration: Second Edition, Revised and Expanded*, edited by Ali Farazmand
95. *Financial Planning and Management in Public Organizations*, Alan Walter Steiss and 'Emeka O. Cyprian Nwagwu
96. *Handbook of International Health Care Systems*, edited by Khi V. Thai, Edward T. Wimberley, and Sharon M. McManus
97. *Handbook of Monetary Policy*, edited by Jack Rabin and Glenn L. Stevens
98. *Handbook of Fiscal Policy*, edited by Jack Rabin and Glenn L. Stevens
99. *Public Administration: An Interdisciplinary Critical Analysis*, edited by Eran Vigoda
100. *Ironies in Organizational Development: Second Edition, Revised and Expanded*, edited by Robert T. Golembiewski
101. *Science and Technology of Terrorism and Counterterrorism*, edited by Tushar K. Ghosh, Mark A. Prelas, Dabir S. Viswanath, and Sudarshan K. Loyalka

Additional Volumes in Preparation

Principles and Practices of Public Administration, edited by Jack Rabin, Robert F. Munzenrider, and Sherrie M. Bartell

Handbook of Developmental Policy Studies, edited by Stuart S. Nagel

Strategic Management for Public and Nonprofit Organizations, Alan Walter Steiss

Case Studies in Public Budgeting and Financial Management, edited by Aman Khan and W. Bartley Hildreth

Annals of Public Administration

1. *Public Administration: History and Theory in Contemporary Perspective*, edited by Joseph A. Uveges, Jr.
2. *Public Administration Education in Transition*, edited by Thomas Vocino and Richard Heimovics
3. *Centenary Issues of the Pendleton Act of 1883*, edited by David H. Rosenbloom with the assistance of Mark A. Emmert
4. *Intergovernmental Relations in the 1980s*, edited by Richard H. Leach
5. *Criminal Justice Administration: Linking Practice and Research*, edited by William A. Jones, Jr.

To the professionals who risk their lives daily in combating terrorism.



Preface

Terrorist activities on the global scene are on the increase, and it is generally believed that such activities can be contained or eliminated by controlling the proliferation of nuclear, biological, and chemical (NBC) weapons, by building a strong defense system, by treaties of different types, and by punishing countries that fail to follow such agreements. One may ask why these procedures, which are in place at the present time, failed to stop activities such as the Tokyo subway gassing, the Oklahoma City bombing, the World Trade Center bombing and attack, the Atlanta Olympic games bomb, and many more. This book is a direct outcome of several recent group discussions by the editors. These meetings were motivated by the fact that some of us are involved in research in the area of sensors, and that one of us (MAP) was spending a year at the State Department as a Foster Fellow. Another motivation was the fact that the Nuclear Engineering program had organized a series of seminars on Non-Proliferation of Nuclear Materials and Weapons in 1998. This series included presentations from Dr. Sudarshan Loyalka, Dr. Mark Prelas, Dr. Dale Klein (currently Assistant Secretary of Defense for NBC Defense), LTC Charles Kelsey, and Dr. Herb Tillema. A major motivation was to introduce undergraduate and graduate students from several disciplines to this important area with an emphasis on the scientific and technological aspects. All these led us to organize and offer courses in the area of terrorism and counter terrorism. One us (DSV) surveyed courses offered in this area in other engineering departments and found that most courses in this area were confined to social, behavioral, and law departments. We could not find a course on the scientific and technological aspects of this subject. Therefore during the fall 2000 semester we organized this course and sought the help of other faculty members. DSV took on the responsibility of drawing up the syllabus and arranging the lectures, and two other editors (MAP and TKG) took the responsibility of taping the lectures, getting the material onto CDs and putting the lectures on the Web (<http://prelas.nuclear.missouri.edu/NE401/NE401.htm>).

The first defense with regard to several areas such as pollution control, waste management, terrorism, and a host of others is education. First it is important to educate a core group – the students who can spread the word. We received good response from the student community. Our thinking that students from various departments should take this course was amply rewarded. The class had stu-

dents from political science, journalism, microbiology, nuclear engineering, mechanical engineering, computer science and computer engineering, and electrical engineering, as well as some with undeclared majors. The class was a 50–50 mix of graduate and undergraduate students. This mix allowed room for extended discussions, and the faculty and students felt that this was one of the strengths of the course. The course received substantial amount of press, radio and TV coverage both locally and on a national scale. We are glad to see that our efforts have culminated in this book form. The enthusiasm of the faculty, students, and the press was overwhelming. Our sincere thanks to all these groups.

We hope that this book will help students who will be our future policy makers and diplomats to understand some basic information on the nature of terrorism, the materials used by terrorists, how to detect them, and how to destroy such materials, and at the same time how to deal with the terrorist groups. We also anticipate that this book will help our current politicians and policy makers. We hope that it will be a catalyst for several engineering departments to offer innovative courses in this area, and enhance our capabilities in counter terrorism.

The book has 26 chapters and the bulk of the material is directed towards understanding the why, how and what of each type of terrorism. It is possible to expand and combine each of the nuclear, biological, chemical and cyber-terrorism chapters with emergency procedures and develop the material into a three-hour course. To appeal to a wider audience, an attempt has been made to streamline both the political and technological parts of terrorism and counter terrorism. We hope this monograph will inspire faculty to innovate courses encompassing several disciplines and to give a broad perspective to the students. The future in this area is unknown as we cannot predict where and when a terrorist strikes, but hope to take all preventive measures to minimize the disaster.

Chapters 2 and 3 lay the foundation for the book by discussing the origin and nature of terrorism, and the factors involved in diplomacy. Chapter 4 deals with the fundamentals of aerosol dispersion as many of the toxic materials are released as aerosol particles. Chapters 5 to 10 deal with the fundamentals of bioterrorism, manufacture of certain biological agents and their delivery. In addition these chapters deal with the detection of biological agents and counter measures. Nuclear terrorism is dealt with in Chapters 11 to 15. Besides discussing the fundamentals, these chapters also discuss nuclear weapons systems, threats, and safeguards. Chapter 16 deals with cyber terrorism. This chapter deals with the nature and scope of cyber terrorism, how cyber terrorism takes place and its consequences, and what we can do to protect against such attacks. Chemical terrorism is described in Chapters 17 to 21. These chapters discuss various chemicals used, their manufacture, detection, delivery, and decontamination. When a disaster occurs, one simple but very effective measure is to protect ourselves with proper clothing. This is discussed in Chapter 22. The role of the government at the federal and state levels and international agencies, their respective resources, capabilities, and responsibilities are discussed in Chapters 23 to 25. One of the most important

aspects of bioterrorism is the prompt identification of its effects. Chapter 26 discusses the role of emergency room personnel in diagnosing a bioterrorism event.

Today we know that citizens have to be very vigilant, and should learn as much as possible about terrorism. The September 11, 2002, World Trade Center attack has awakened the country like no other single event in the history of the US, presumably not even the Pearl Harbor attack. The public needs to know the profile of a terrorist; the threat of nuclear, biological, and chemical weapons; what measures to take in case of an attack; how to respond in case of an emergency; and a host of other things. We have tried to present as comprehensive a report as possible. We recognize that we have not covered all the materials that should be included in a text of this nature. Parts of the book can be expanded to present more comprehensive courses.

In closing, it is a pleasure to thank the faculty and guest lecturers who willingly participated in the course, contributors to this book who in spite of their busy schedules cooperated in getting the manuscript completed in a short time, students who participated in the course and whose enthusiasm encouraged the faculty to do their best, the local and national media who interviewed us about this course, the reviewer for the comments which significantly improved the presentation, and Marcel Dekker, Inc., for their help and cooperation. Additionally, this text is the first manuscript from the newly formed Nuclear Science and Engineering Institute at the University of Missouri-Columbia. We wish to express our gratitude to the University of Missouri.

Tushar K. Ghosh
Mark A. Prelas
Dabir S. Viswanath
Sudarshan K. Loyalka



Acknowledgements

Tushar Ghosh thanks his wife Mahua for her encouragement, patience and understanding throughout the writing of the book. He also thanks his son Atreyo and daughter Rochita for their understanding and patience.

Mark Prelas especially thanks his family, Rosemary S. Roberts (his wife and the love of his life), Natalia (his daughter) and Alexander (his son) for their patience. He also thanks his colleagues from the US Department of State's Bureau of Arms Control, Dr. Robert Gromell, Dr. Peter Almquist, Dr. Eric Arnett, Dr. Chaitan Gupta, Colonel Kenneth Hodgdon, Colonel John Kyme, Colonel John Riley and Mr. Mike Flores for their enthusiasm and encouragement for this project.

Dabir Viswanath thanks his wife Pramila and his son Arvind for their patience, support and encouragement.

Sudarshan Loyalka thanks his family, friends, students and colleagues (especially the other three editors and the chapter authors) for their support and encouragement during the writing of this book.

Contents

<i>Preface</i>	v
<i>Contributors</i>	xiii
1 Introduction <i>Dabir S. Viswanath</i>	1
2 A Brief Theory of Terrorism and Technology <i>Herbert K. Tillema</i>	13
3 The Group Psychology of Terrorism <i>Michael A. Diamond</i>	35
4 Aerosols: Fundamentals <i>Sudarshan K. Loyalka and Robert V. Tompson, Jr.</i>	47
5 Biological Agents: Effects, Toxicity, and Effectiveness <i>Gordon D. Christensen</i>	61
6 Weaponization and Delivery Systems <i>Mark A. Prelas</i>	95
7 The Classification and Manufacture of Biological Agents <i>Mark A. Prelas</i>	109
8 Agroeconomic Terrorism <i>Keith A. Hickey</i>	121
9 Sensors and Detection Systems for Biological Agents <i>Tushar K. Ghosh and Mark A. Prelas</i>	145
10 Bioterrorism: Preparation for Response – What the Government Can Do in Defending the Homeland <i>Marion C. Warwick</i>	195
11 Nuclear Terrorism: Nature of Radiation <i>William H. Miller</i>	259
	xi

xii	Contents
12 Nuclear Terrorism: Radiation Detection <i>William H. Miller</i>	265
13 Nuclear Terrorism: Dose and Biological Effects <i>William H. Miller and Robert Lindsay</i>	269
14 Nuclear Terrorism: Nuclear Weapons <i>Sudarshan K. Loyalka</i>	277
15 Nuclear Terrorism: Threats and Countermeasures <i>Sudarshan K. Loyalka and Mark A. Prelas</i>	285
16 Cyber-terrorism <i>Harry W. Tyrer</i>	293
17 Chemical Agents: Classification, Synthesis and Properties <i>Dabir S. Viswanath and Tushar K. Ghosh</i>	321
18 Chemical Agents: Toxicity and Medical Management <i>L. David Ormerod</i>	345
19 Chemical Weapon Delivery, Sensors and Detection Systems <i>Mark A. Prelas and Tushar K. Ghosh</i>	373
20 Chemical Agents: Destruction and Decontamination <i>Dabir S. Viswanath and Tushar K. Ghosh</i>	411
21 Chemical Agents: Threats and Countermeasures <i>L. David Ormerod, Tushar K. Ghosh, and Dabir S. Viswanath</i>	429
22 Personal Protective Equipment <i>Glenn P. Jirka and Wade Thompson</i>	447
23 The National Response Plan <i>Julie A. Bentz</i>	465
24 Emergency Response and Training <i>Robb L. Pilkington</i>	489
25 Government and Voluntary Agencies <i>Julie A. Bentz</i>	507
26 Bioterrorism: Consequences and Medical Preparedness <i>L. David Ormerod</i>	527
<i>Index</i>	561

Contributors

Julie A. Bentz is a nuclear medical science officer at the National Guard Bureau (NGB) in the office of Civil Support. This office manages the National Guard Civil Support Teams (CSTs) who act as the governor's "911" response element for Weapons of Mass Destruction (WMD) events. A member of the National Inter-agency Technical Support Working Group and the WMD Civil Support Test Integration Working Group, MAJ Bentz serves as an interface of emerging technology and the needs of the first responders. Her responsibilities include equipping and sustaining the CSTs as well as serving as science advisor and combat developer in which position she authored the current Civil Support Operational and Organizational Plan and the Operational Requirements Document for CST Equipment. Dr. Bentz received the Ph.D. degree (1999) in nuclear engineering from the University of Missouri-Columbia.

Gordon D. Christensen is the Associate Chief of Staff for Research and Development at the Harry S Truman Memorial Veterans Hospital in Columbia Missouri and a Professor of Internal Medicine at the University of Missouri-Columbia. He is a Fellow of the Infectious Diseases Society of America, the American Academy of Microbiology, and the American College of Physicians. He is the author or co-author of over 120 professional papers and abstracts. He received his M.D. degree (1974) from Creighton University in Omaha, Nebraska and he completed his post-graduate training in infectious diseases and internal medicine (1979) at the University of Texas Medical Branch in Galveston, Texas.

Michael A. Diamond, Ph.D. is Professor of Public Affairs and Organizational Change and Director of the Center for the Study of Organizational Change at the Harry S Truman School of Public Affairs, University of Missouri-Columbia, where he teaches, writes, and consults on organizational analysis and change. Dr. Diamond is author of *The Unconscious Life of Organizations: Interpreting Organizational Identity* (1993) and co-author of *The Human Costs of a Management Failure* (1996) and *Managing People During Stressful Times* (1997), Quorum Books, Greenwood Publishing. He has published widely in scholarly journals and was co-editor-in-chief of the *American Review of Public Administration* from 1987 to-1995. In 1994 he was awarded the Harry Levinson Award for Excellence

in Consulting Psychology from the American Psychological Association and won the prestigious 1999 William T. Kemper Fellow for Excellence in Teaching from the University of Missouri-Columbia. He is founding member and past-president of the International Society for the Psychoanalytic Study of Organizations and visiting faculty for INSEAD (Fontainebeau, France) and HEC (Jouy-en-Josas, France) International Diploma Program in Consulting and Coaching for Change. He is also a member of the American Psychological Association (Psychoanalysis and Consulting Psychology divisions) and the International Society of Political Psychology.

Tushar K. Ghosh is an Associate Professor in Nuclear Engineering at the University of Missouri-Columbia (MU). Following graduation with a Ph.D. degree in Chemical Engineering in July 1989, from Oklahoma State University in Stillwater, OK, he worked at MU as a Research Assistant Professor in conjunction with the Chemical and Nuclear Engineering departments and the Particulate Systems Research Center. He was responsible for building several pieces of equipment that are currently being used in the Indoor Air Research Laboratories. His present research interests include enhancement of indoor air quality by adsorption and absorption processes, measurement and removal of radon from indoor air, and particle production/synthesis.

Keith A. Hickey is the Medical Physicist and Radiation Safety Officer at Missouri Cancer Associates, and is an Adjunct Assistant Professor at the University of Missouri. A member of the American Association of Physicists in Medicine, the Health Physics Society and the Institute of Electrical and Electronics Engineers, Dr. Hickey is a Certified Health Physicist and is board certified by the American Board of Radiology in Therapeutic Radiological Physics. A former U.S. Army Reserve Nuclear Medical Science Officer with several years' experience in defense advanced technology and systems engineering, Dr. Hickey received the Ph.D. degree (1989) in nuclear engineering from the University of Missouri-Columbia.

Glenn P. Jerka is the Environmental Emergency Response Program Manager for the University of Missouri-Columbia Extension Division's Fire and Rescue Training Institute and an Adjunct Assistant Professor in the College of Engineering at the University of Missouri-Columbia. A member of the National Fire Protection Association Technical Committee on Hazardous Materials Protective Clothing and Equipment, the Department of Justice--Department of Defense joint Interagency Board for Equipment Standardization and Interoperability, and the Federal Emergency Management Agency's First Responder Technology Transfer Committee on Weapons of Mass Destruction and Hazardous Materials, among others, he is the author or coauthor of numerous professional papers and curricula. Mr. Jerka received the M.S. degree (1990) in chemistry from Southern Illinois University-

Carbondale and completed post-graduate work with the School of Chemical Sciences at University of Illinois Urbana-Champaign.

Robert Lindsay is an Associate Professor in the Physics Department at the University of the Western Cape in South Africa. He was awarded a Rhodes scholarship in 1978 for study at Oxford in England after obtaining a B.Sc. degree in Physics at Stellenbosch University in South Africa. He obtained a D.Phil in Theoretical Physics at Oxford in 1982. He spent two years as a post-doc at Daresbury Laboratory in the UK and then joined the University of the Western Cape. His present research interests are in applied nuclear physics, specifically radon measurements and the use of natural radioactivity.

Sudarshan K. Loyalka is a Curators' Professor of Nuclear Engineering and Chemical Engineering and is Director of the Particulate Systems Research Center at the University of Missouri-Columbia. His research interest are in transport theory, aerosol mechanics, the kinetic theory of gases, and neutron reactor physics and safety. Dr. Loyalka is a Fellow of both the American Physical Society (since 1982) and the American Nuclear Society (since 1985). He has published more than 170 papers and advised approximately 70 graduate students. He has received numerous awards for his research and teaching including the David Sinclair Award (1995) of the American Association for Aerosol Research and the Glenn Murphy Award (1998) of the American Association for Engineering Education.

William H. Miller is the James C. Dowell Research Professor of Nuclear Engineering and Director of the Energy Systems and Resources Program at the University of Missouri-Columbia, where he has taught graduate nuclear engineering for 28 years. He is the author of approximately 100 papers and has made over 1000 presentations to the public on issues concerning energy, the environment, radiation and nuclear power. He received his Ph.D. in Nuclear Engineering from the University of Missouri-Columbia.

L. David Ormerod, M.D. was until recently Chief of Vitreoretinal Surgery and Associate Professor of Ophthalmology at the University of Missouri-Columbia School of Medicine. Educated at St. Bartholomew's Hospital Medical College, University of London, he is a Fellow of the Royal College of Surgeons, Fellow of the Royal College of Ophthalmologists, and Member of the Royal College of Physicians. His is a diplomate in Tropical Medicine and Hygiene (London School of Hygiene and Tropical Medicine) and has a M.S. Immunology degree from the University of Birmingham (UK). Professional service includes the Hospital for Tropical Diseases, London, and Ahmadu Bello University, Zaria, Nigeria. Dr. Ormerod is US fellowship-trained in cornea and external diseases (Harvard University) and in the retina (Wayne State University) and has received the Honor Award of the American Academy of Ophthalmology. He is the author of 85 publi-

cations in ophthalmology, internal and tropical medicine, immunology, visual rehabilitation, and the medical aspects of terrorism.

Robb Pilkington is the counter terrorism program manager for the University of Missouri Fire and Rescue Training Institute and an Adjunct Assistant Professor of Nuclear Engineering. He manages course deliveries and develops specialized courses for first responders, government agencies and public officials. Robb is a member of the Interagency Board (IAB) for Detection and Decontamination, the International Association of Emergency Managers, and the Missouri Homeland Defense Responders Subcommittee. Robb is a member of Missouri Task Force-One Urban Search and Rescue Team and is a Hazardous Materials Response Specialist. He has completed doctoral degree coursework (ABD) at Oregon State University in Corvallis; and an M.S. from the University of Missouri (1978).

Mark A. Prelas is H. O. Croft Professor of Nuclear Engineering at the University of Missouri-Columbia. Dr. Prelas received his Ph.D. from the University of Illinois in 1979. He received the Presidential Young Investigator Award in 1984, was a Gas Research Institute Fellow in 1981, was a Fulbright Fellow at the University of New South Wales in 1992, was named a fellow of the American Nuclear Society in 1999 and was a William C. Foster Fellow with the U.S. Department of State in 1999–2000. In addition to being a professor at the University of Missouri, he worked at the U.S. Department of State in the bureau of Arms Control in 1999–2000 and with the Idaho National Engineering Laboratory of the U.S. Department of Energy in 1987. He has worked in the areas of arms control for weapons of mass destruction, in the development of nuclear, chemical and biological sensors, in the synthesis and applications of wide band-gap materials, in directed energy weapons, in direct energy conversion and in gaseous electronics. He has published over 200 papers and 5 books, and holds 12 national and international patents.

Wade Thompson is an Adjunct Associate Instructor for the University of Missouri-Columbia Extension Division's Fire and Rescue Training Institute. He is also a Lieutenant with the Columbia, MO Fire Department, a member of the WMD response unit housed at the Boone County (MO) Fire Protection District, and a former member of the United States Marine Corps Second Recon Battalion. Mr. Thompson has over ten years' experience in hazardous materials and emergency response.

Herbert K. Tillema is Professor of Political Science at the University of Missouri-Columbia. Academic degrees include: B.A., Hope College, 1964; and Ph.d. Harvard University, 1969. He served as Commissioner, State of Missouri Peace Officer Standards and Training Commission, 1992-1994. He is author of books and articles on the use of force in international relations, including: *Appeal to Force- American Military Intervention in the Era of Containment*; and *International Armed Conflict Since 1945*.

Dr. Robert V. Tompson, Jr. is an Associate Professor of Nuclear Engineering in the Nuclear Science and Engineering Institute (NSEI) at the University of Missouri-Columbia (MU). He received his BS in physics (1980), his M.S. in nuclear engineering (1984), and his Ph.D. in nuclear engineering (1988); all from MU. He subsequently worked for three years as a post-doctoral research associate; first at the University of Kentucky for one year and then back at MU for two more years. Dr. Tompson was the recipient of a NASA Summer 1991 Faculty Fellowship at the Langley Research Center, following which he became a tenure-track assistant professor at MU. Dr. Tompson is deeply involved in the activities of the Particulate Systems Research Center (PSRC) at MU where he is the Associate Director. His research interests are in the experimental and theoretical aspects of nuclear reactor safety, aerosol mechanics, rarefied gas dynamics, indoor air quality, particulate-based and related materials, and particle manufacturing and applications. He is a member of the American Nuclear Society (ANS), the American Physical Society (APS), the American Vacuum Society (AVS), the American Association for Aerosol Research (AAAR), the Society for Industrial and Applied Mathematics (SIAM), and Sigma Xi. As of 2002, Dr. Tompson has about 70 publications including almost 40 refereed journal articles as well as a number of transactions and proceedings.

Harry W. Tyrer is Professor and Chairman of the Computer Engineering and Computer Science Department at the University of Missouri-Columbia. His degrees are all in electrical engineering with a Ph.D. (1972) from Duke University. He has edited 3 volumes and several special journal issues. He has contributed to over 60 publications. He has developed biomedical instrumentation, object oriented applications, and wireless communication systems. Additionally he has written on real time operating systems, digital systems, computer networks, and computer network performance.

Dabir S. Viswanath is Emeritus Professor and Dowell Chair of Chemical Engineering, University of Missouri-Columbia. Since his retirement in 2000, Dr. Viswanath has been associated with the Nuclear Science and Engineering Institute at the University. He is a Fellow of both the American Institute of Chemical Engineers and the American Institute of Chemists. He has advised over 50 graduate students, and has published over 130 peer reviewed papers and 4 American Petroleum Institute monographs. He co-authored *Data Book on the Viscosity of Liquids* published by Hemisphere in 1989. His research interests are in thermodynamic properties and transport of liquids and gases, process development, wastewater treatment, and thermal degradation of polymers in ceramics. He has taught at Bucknell University, Indian Institute of Science, and Texas A & M.

Marion Warwick is a Medical Epidemiologist and the Bioterrorism Coordinator for the Missouri Department of Health and Senior Services. Board certified in both family practice and preventive medicine, she currently practices medicine, is the

author of several papers on subjects related to both medicine and public health, and is a member of the American Society of Tropical Medicine and Hygiene. She received the M.D. degree from the University of Minnesota (1985) and the M.P.H. degree from the University of Massachusetts, Worcester (1996).

Science and Technology
of Terrorism and
Counterterrorism

1

Introduction

Dabir S. Viswanath

University of Missouri, Columbia, Missouri

SUMMARY

The Rand Report [1] under the Chairmanship of Governor Gilmore of Virginia stated that “The United States needs a functional, coherent national strategy for domestic preparedness against terrorism. Administrative measurements of program implementation are not meaningful for the purposes of strategic management and obscure the more fundamental and important question: To what end are these programs being implemented? The Advisory Panel therefore recommends that the next President develops and presents to the Congress a national strategy for combating terrorism within one year of assuming office. As the Advisory Panel recognized in its first report, our nation’s highest goal must be the deterrence and prevention of terrorism. The United States cannot, however, prevent all terrorist attacks”.

The programs recommended by the Panel are:

“Domestic Preparedness Programs: We recommend an Assistant Director for Domestic Preparedness Programs in the National Office to direct the coordination of Federal programs designed to assist response entities at the local and State levels, especially in the areas of “crisis” and “consequence” planning, training, exercises, and equipment programs for combating terrorism. The national strategy that the National Office should develop — in coordination with State and local stakeholders — must provide strategic direction and priorities for programs and activities in each of these areas.

Health and Medical Programs: Much remains to be done in the coordination and enhancement of Federal health and medical programs for combating terrorism

and for coordination among public health officials, public and private hospitals, pre-hospital emergency medical service (EMS) entities, and the emergency management communities. We recommend that the responsibility for coordinating programs to address health and medical issues be vested in an Assistant Director for Health and Medical Programs in the National Office for Combating Terrorism. The national strategy should provide direction for the establishment of national education programs for the health and medical disciplines, for the development of national standards for health and medical response to terrorism, and for clarifying various legal and regulatory authorities for health and medical response.

Research, Development, Test, and Evaluation (RDT&E), and National Standards: We recommend that the responsibility for coordinating programs in these two areas be assigned to an Assistant Director for Research, Development, Test, and Evaluation, and National Standards in the National Office for Combating Terrorism. The national strategy should provide direction and priorities for RDT&E for combating terrorism. We believe that the Federal government has primary responsibility for combating terrorism RDT&E. Local jurisdictions and most states will not have the resources to engage in the research and development required in the sophisticated environment that may be a part of the nation's response to terrorism. Moreover, we have essentially no nationally recognized standards in such areas as personal protective equipment, detection equipment, and laboratory protocols and techniques."

Thus the report clearly points to the fact that counter terrorism measures must be developed and should be in place, and that research, development, testing and evaluation must be supported. In order to carry out significant research in any area students must be educated and the future research needs explored. It was with this objective in mind that we developed a curriculum in the area of Scientific and Technological Aspects of Terrorism and Counter Terrorism. Our search for courses that dealt with the scientific and technological aspects of terrorism and counter terrorism revealed that the engineering and science departments did not teach any course of this nature, but a large number of courses were taught by faculty in political science, public policy, and related areas. The motivation to start a program of this type was enhanced when we found that there are hundreds of books, and a host of journals dealing with this subject; however, the scientific and technological aspects of Terrorism and Counter Terrorism are loosely and thinly spread in some journal articles as for example in the August 1997 [Volume 278, No. 5] issue of the Journal of American Medical Association on biological warfare.

As of this writing, President George W. Bush has formed the Office of Homeland Security under the leadership of Governor Tom Ridge. This is discussed in later chapters.

The Five-Year Interagency Counter-terrorism and Technology Crime Plan [2] lists specific goals that are to be addressed. They are to:

1. identify critical technologies for targeted research and development efforts;
2. outline strategies for preventing, deterring, and reducing vulnerabilities to terrorism and improving law enforcement agency capabilities to respond to terrorist acts while ensuring interagency cooperation;
3. outline strategies for integrating crisis and consequence management;
4. outline strategies to protect our national information infrastructure; and
5. outline strategies to improve state and local capabilities for responding to terrorist acts involving bombs, improvised explosive devices, chemical and biological agents, and cyber attacks.

Education and research are key components in combating terrorism. In order to have a better understanding of terrorism and then to counter it one should understand:

1. the psychology of the terrorist or terrorist groups, the prevailing atmosphere in some countries which encourage and promote terrorist activities, and the religious, cultural and economic background,
2. how to manage the terrorist events, and the short- and long-term effects of terrorist acts,
3. what measures have to be taken to prevent terrorist acts. This involves educating both the terrorist (which is not easy) and the victim,
4. the underlying details of the weapons used in NBCC (Nuclear, Biological, Chemical, and Cyber) acts so that counter measures can be devised.

Terrorism by nature is difficult to define. Even the U.S. government cannot agree on one single definition. The old adage, "One man's terrorist is another man's freedom fighter" is still alive and well. Listed below are several definitions of terrorism.

Terrorism is the use or threatened use of force designed to bring about political change. Laqueur [3] defines terrorism as an act, which constitutes the illegitimate use of force to achieve a political objective when innocent people are targeted.

According to Poland [3], terrorism is the premeditated, deliberate, systematic murder, mayhem, and threatening of the innocent to create fear and intimidation in order to gain a political or tactical advantage, usually to influence an audience.

The Vice President's Task Force in 1986 defined terrorism as the unlawful use or threat of violence against persons or property to further political or social

objectives [4]. It is usually intended to intimidate or coerce a government, individuals or groups, or to modify their behavior or politics.

According to the FBI, terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

All these definitions have some connotation to political activity. However certain acts such as the poisoning of Tylenol tablets, the bombing of Centennial Olympic games in Atlanta, and a score of others do not lend themselves to any political motives. Therefore a much more general definition seems in order which should include non-political aspects of a terrorist act.

Some of the terrorist acts that have taken place during the past few years can help in understanding the complexity of this subject. A collection of case studies can help identify the following:

- The type of people involved in terrorist attacks.
- The types of weapons used in these attacks.
- Possible motives behind such attacks.
- Whether any information was available before such attacks and what action, if any, was taken.
- What measures have been taken to prevent such attacks in future, and
- Where should the resources be spent to maximize the benefit.

From 1990 to 1998, terrorism in the United States has increased steadily [5], and a history of these events is shown in Table 1.1.

During 1997 and 1998, the number of cases or threats investigated on WMD are: nuclear 25, 20; chemical 20, 23; and biological 22, 112; others 7, 17, respectively. Although the nuclear threat has come from the breakup of the Soviet Union and clandestine removal of nuclear materials, the number of chemical and biological threats has also increased several fold. We will outline some of the chemical and biological threats, and try to raise questions. We will not discuss the details of the attacks, as the primary focus is to generate questions resulting from these incidents.

Based on the data given above, the free flow of information, religious fundamentalism, increasing lethality of current biological and chemical weapons, the ease with which terrorist groups can acquire or develop weapons, and other factors, it can only be surmised that the number of terrorist activities will increase and cause more damage. However, in spite of the availability of technology in the open literature, as it is not easy for the terrorists to manufacture biological and chemical weapons, timely action might prevent terrorist activities and could be a lesson for others. At the same time it is important to understand that the current political unrest in various parts of the world, and the economic disparity between the haves and the have-nots are drawing more and more educated people, and this is a cause for alarm. This will help in the faster implementation of the technology available in the open literature. Thus it is a fairly complex issue, and an increased

vigilance on the part of all citizens is important to reduce terrorist activities. This increased vigilance can come by educating the public and through their efforts.

We would like to present a brief study of six terrorist acts that have occurred in the recent times. We hope an in-depth study of these case studies will reveal the inherent problems in the design of the security management, weaknesses in the design of such security management systems, adequacy or inadequacy of response, interface requirements such as sharing intelligence among various groups/agencies or even countries in combating terrorism, deep understanding of religious and cultural aspects, profiling of terrorists and terrorist organizations, and a host of other questions.

Table 1.1 A listing of terrorist events in the United States from 1990 to 1999.

Year	Incidents	Suspected Incidents	Prevention
1990	7	1	5
1991	5	1	5
1992	4	0	0
1993	12	1	7
1994	0	1	0
1995	1	1	2
1996	3	0	5
1997	2	2	20
1998	5	0	12
1999	10	2	7

Source: Federal Bureau of Investigation, National Security Division, Terrorism in the United States, Report, 1998, 1999 [5].

WORLD TRADE CENTER (WTC) BOMBING

On February 26, 1993, a car bomb exploded at the B2 level of WTC killing six persons and injuring hundreds. The blast created a six-meter diameter hole. The event posed a number of questions.

1. What kind of intelligence did the government have about this attack? Was the attack instrumental in getting through a quick passage of the 1995 Counter Terrorism Bill?
2. Was this a Stateless warfare? If so, how can a government protect its citizens?
3. How many states or countries can the US punish in order to contain such attacks? Would this work?
4. Is this a deep psychological problem?

5. Is this a religious problem? Do we know the basic tenets of different religions, and which ones can we trust?
6. Why do terrorists target the U.S. and citizens of the U.S.? Can we draw broad based conclusions and/or correlations of the different terrorist attacks based on the policies of the U.S. at different times and support given to different types of governments and people?

TOKYO SUBWAY ATTACK

The Tokyo subway attack by Aum Shinrikyo, or Supreme Truth, cult occurred on March 20, 1995, and killed over a dozen people and injured more than 5,000. The chemical used in this attack was sarin gas (GB), although there were indications that the group was experimenting with biological agents such as anthrax, botulism toxin, and Ebola virus. There were widespread reports that this was a trial attack by the Aum group before a larger attack, and that the Aum group experimented with sheep in the Banjawarn area in Australia. The latter news was based on an Australian Broadcasting Company report and was thought to be incorrect for various reasons, and the European experts in chemical and nerve gas detection laughed at the suggestion that experiments on sheep were carried out with sarin. Aum members in this Australian ranch were apparently warned of a police attack. There are hundreds of reports and writings on this incident just like the Oklahoma Federal Building attack or the World Trade Center attack. What important lessons can we learn from this Tokyo subway incident? Besides the points raised above in the Oklahoma attack, some other points are:

1. Sarin was the chemical used, and like sarin there are many other nerve gases and toxic chemicals. Have we reached a time when some of the chemicals should be restricted, even if they are of commercial importance?
2. Should we pay more attention to the reports, such as that of Australian Broadcasting Company, and investigate more thoroughly?
3. Should there be more financial commitment for research and development in areas such as sensor technology?
4. In the event of an attack, what is the minimum amount of information the public should know to defend or help them?
5. What was the motive of Aum Shinrikyo?
6. Will chemicals like sarin create allergy problems? How will one answer this question? Should there be research in this area?
7. Are the components of chemical and biological weapons available too easily?
8. How far can we go in preventing proliferation of biological and chemical weapons?

OKLAHOMA CITY BOMBING

On April 19, 1995, a bomb destroyed the Alfred Murrah Federal Building in Oklahoma City, and killed 168 people and injured hundreds more. Several agencies and teams were involved in the investigation. These agencies were ATF, FBI, local police and fire departments, Secret Service, many voluntary groups, and many other independent agencies. The investigation was intense, but from the point of view of terrorism and counter terrorism, what are the important factors and what lessons have we learned?

The bomb was made with approximately two tons of ammonium nitrate fertilizer mixed with combustible fuel oil, and it was taken in a Ryder truck, and parked in front of the north side of the building before it was detonated. Some questions are:

1. Was the building designed to withstand such blasts?
2. Should a chemical like ammonium nitrate be restricted? If so, what about ammonia and nitric acid? Can terrorists get hold of chemicals sold normally in the open market and make destructive chemicals?
3. How did the morale of the people in the country and around the world suffer? What was the impact on the people in the city, and what type of psychological counseling should be provided? What are the political implications? At first it was thought that a Middle-Eastern group had carried out this attack, particularly in view of the World Trade Center bombing on February 26, 1993. What would have happened if McVeigh was not arrested quickly?
4. What type of response was available immediately after the bombing – emergency, medical, etc? Was it satisfactory? In public buildings where a large number of people work, should there be a common area where all personnel are required to go to report to get further instruction before leaving the building? Should most of the people in that building receive EMT training? How about communications, etc?
5. In Oklahoma City, WTC, and USS Cole bombings, vehicles were involved. Should there be restrictions regarding the vehicular traffic (to keep them at a distance from the buildings), plans to transport materials that arrive at the building (unload from the carrying vehicle to a vehicle owned by the Security at the building), etc.?
6. In these situations, the FBI and FEMA had the control. Would this hinder the assistance efforts of other organizations such as Red Cross, church organizations, etc? How should the relief efforts be coordinated? What type of measures should be in place for issuing identifications, etc.? The President signed an emergency declaration within 8 hours of the occurrence-the first time section 501(b) of the Stafford Act, granting FEMA the primary federal responsibility for responding to a domestic conse-

quence management incident, was activated. The President subsequently declared a major disaster on April 26, 1995.

INTERNAL TERRORISM: REPUBLIC OF TEXAS (TERRORIST ACTIVITIES OF WISE, GREBE, AND EMIGH)

Political objectives and motives appear to be the major reasons for terrorist activities. Almost all national or international terrorist attacks can be traced to political ends. In some of the cases, it is not clear how far the authorities follow tips or information to crack down on terrorist groups. This particular incident reveals how one attack was prevented.

Three men belonging to the Republic of Texas group, Johnny Wise, Jack Abbott Grebe, Jr., and Oliver Dean Emigh, plotted to kill several members of the government including President Clinton. They were to obtain anthrax from external sources outside the country, and were trying to make devices to target a federal judge in Texas. Fortunately, FBI agents arrested these suspects on July 1, 1998. The FBI acted quickly in this case and thus prevented what could have been a major catastrophe. The trial of this case began on October 19, 1998 and concluded on October 29, 1998 when two of the three were convicted. What can we learn from this episode?

1. Did the FBI act timely to nab the perpetrators?
2. Under what circumstances would the FBI think that a report is credible or not? In this case, it is reported that an FBI agent did not think that the "alleged plot to assassinate government officials with poisoned cactus needles shot out of Bic lighters was far-fetched."
3. What type of devices did this group put together? The lighters were to be rigged to shoot cactus needles dipped in substances such as anthrax, AIDS-tainted blood and rabies, according to an account by federal officers.
4. Where did they get information to make the devices they were trying to assemble?
5. Are the regulations for importing materials adequate?
6. If they succeeded in getting anthrax from a foreign source, what could have been the consequences?
7. Are they part of a larger group, and if so what measures have been taken to keep a watch on this group?
8. Did the investigation end with their conviction or did it continue? If it continued, was the public informed?
9. What is the profile of these people? Can the citizens be familiarized with these profiles, and be guarded?
10. Were there any psychological tests carried out to profile the type of individuals who could carry out such threats?

11. What is their educational background, and did they understand what they were up to?
12. What measures are in place to disseminate information? Should this information be disseminated at all?
13. How far can the government go before constitutional rights are violated?

SECOND WORLD TRADE CENTER ATTACK

On September 11, 2001, two jets from Boston—one bound to Los Angeles and the other one to San Francisco—were crashed into Towers 1 and 2 of the WTC. In all, four passenger jets were involved in different attacks on that day, killing over 3,000 persons. In addition, the immediate economic losses to the City of New York could be as high as 30 billion dollars, and the long-term economic losses to the U.S. could amount to hundreds of billions of dollars.

The loss of life in this attack was heavy, and mostly unaccounted. Simple calculations show temperatures in excess of several thousand degrees could have resulted inside the tower building. The towers, 415.5 m (1363.25 ft) and 417 m (1368.2 ft) tall, housed 418,600 m² (4,504,136 ft²) of office space. The airplanes that hit the WTC were Boeing 767 and 757. Taking aviation fuel as a saturated hydrocarbon, and assuming that less than 5% of the total fuel (approximately 63210 liters or 16,700 gallons) burned in an area of 3011 m² (32,400 ft²) (approximate area/floor), the amount of heat generated will be, approximately, 7.6×10^{10} joules (72×10^6 Btu). The air inside a volume of 11,011 m³ (388,800 ft³) (assuming a height of 3.65 m (12 ft) gets heated to more than 5538°C (10,000°F). This is equivalent to a detonation of 490 kg of TNT. It is estimated that the Oklahoma City blast amounted to 82 kg of TNT.

This attack raises several questions besides those raised in the previous cases. We will raise these questions in two sets—one similar to those raised in the examples cited above, and the other set pertaining to long-range policy. The first set of questions is:

1. Is there any thing close to foolproof airport security? What steps should be taken to enhance airport security?
2. It was reported that some of the persons involved in this attack took part in other attacks such as the bombing of USS Cole. These persons were residing in the U.S. without proper documents. Is this a failure on the part of FBI or failure of the INS? Do these agencies work separately? Is there a need for these two agencies to work closely at least in certain cases? Should several departments such as the law enforcement, CIA, FBI, and INS work together? In that case who should be in charge of these departments? Should the Federal government create a separate umbrella to oversee the work of these departments?

3. The New York City Fire Department, hospitals, volunteers, police, and other agencies did a heroic job. Was the emergency preparedness adequate? Do we have the same type of preparedness in other parts of the country as in New York?
4. Do we need new codes for buildings of the type of WTC?
5. We seem to be dealing with a particular set of people in this world who are identified with terrorist acts. Do we have the psychological profiles of the people who commit such terrible terrorist acts? Do we have a deep understanding of their religion and beliefs? Why do these countries, one after another, hate the U.S.?
6. What type of terrorism is this? Is this chemical terrorism?
7. How can the injured and dead bodies be recovered in an organized and respectful way?

The second set of questions is:

1. Why is U.S. the main target of terrorist attack?
2. What is the origin of the persons who carried out this attack?
3. Being the most powerful nation in the world, what should be the U.S. policy towards other countries?
4. President Bush very correctly said "Terrorism in any form is bad." Would this be the cornerstone of the U.S. policy? Can the U.S. boldly follow this principle? Would this jeopardize the U.S. interests in trade and commerce? How far can the U.S. go in sacrificing its standard of living?

ANTHRAX THREAT

Bioterrorism threat has emerged since October of 2001, and anthrax scare came to the U.S. Capitol Hill. The spores of the bacterium were discovered in several places including Senator Daschle's office at the Hart Senate Office building in Washington, D.C.; mail-sorting equipment in Brentwood road, NBC anchor Tom Brokaw's office in New York; the office of a photo editor of Sun tabloid in Boca Raton, Florida; Kansas City, Missouri; and other places. Two postal workers in Washington, D.C. area, Thomas Morris, Jr., and Otilie Lundgren, of Oxford, Connecticut, died due to anthrax inhalation. September 18 to the middle of December 2001 was a very anxious period for all, not knowing how this scare came about and who was responsible. As of May 29, 2002 the FBI has few clues as to who may have created the anthrax scare.

This threat appears to be more at home than a threat due to a chemical weapon, and a host of questions can be asked:

1. How can one find out whether it is anthrax?

2. If exposed to anthrax spores, where should one go?
3. How does one know whether she/he is in a high or low risk category?
4. What precautions should be taken before handling mail?
5. How can the public get information on post offices closed due to anthrax contamination?
6. How can one tell if exposed to cutaneous anthrax?
7. How can one be sure that the mail is not contaminated by anthrax?
8. People who got infected were in different places such as mailrooms, hospitals, and other areas. Did they get infected by mail or by some other method?
9. Are there enough medical facilities to cope with a major threat? How should the health care personnel respond in case of an emergency?
10. What should a person do to get prepared to deal with an anthrax scare?
11. How resistant are the spores?

In 1979, the city of Sverdlovsk in the former Soviet Union experienced an anthrax outbreak. There was a difference of opinion regarding the source of anthrax. While the Soviet Union believed it was from contaminated meat, the U.S. sources maintained that it was due to a leak from the anthrax-manufacturing facility. This epidemic claimed 68 lives and 17 suffered skin infection. In all likelihood, spores of anthrax spread as an aerosol, and affected people close to the manufacturing facility. It is reported that there has been only 18 cases of anthrax between 1900 and 1976 (cnn.com/health, October 5, 2001).

As we see from these six examples, the motivation in all cases appears to be political, one way or other, either internal or external to the state. The profile of the individual or individuals involved has not been analyzed to draw conclusions to help identify future terrorists. Except in the case of the Tokyo subway incident, the individuals involved were not highly educated and technically skilled persons, but had some practical experience. All cases are chemical terrorism in nature, and the chemicals used could be purchased or synthesized. It is evident that the chemicals used have a dual purpose as industrial chemicals and chemicals for terrorist activities.

REFERENCES

1. Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, James S. Gillmore, Chairman, December 15, 2000.
2. The Five-Year Interagency Counter-terrorism and Technology Crime Plan, Attorney General, 1999 Report, February 1, 1999.
3. Terrorism Research Center, Definition Page, 1996-2000. <http://www.terrorism.com/terrorism.def.shtml>.

4. Vice President of the United States. Public Report of the Vice President's Task Force on Combating Terrorism. February, 1986.
5. Federal Bureau of Investigation, National Security Division, Terrorism in the United States, Report, 1998. <http://www.fbi.gov/publications/terror/terroris.htm>.

2

A Brief Theory of Terrorism and Technology

Herbert K. Tillema

University of Missouri, Columbia, Missouri

INTRODUCTION

What and why is terrorism? What can be done about it? Terrorism is undeniably horrific. It kills, maims, and destroys property for political purposes. Few praise terrorism in itself, not now and not in the past. Nevertheless, the practice has persisted for literally thousands of years. In some ways, terrorism is more horrifying than other awful forms of violence, including war, criminal brutality, and psychopathic mayhem, each of which also has a long history. Soldiers in war at least expect violence. Victims of crime at least comprehend violence inflicted for material gain. Those who suffer at the hands of the psychopath may at least attribute loss to fate. Victims and witnesses of terrorist acts, on the other hand, seldom expect the event, cannot easily understand why violence strikes when and where it does, but know that damage is inflicted for a purpose. They are made fearful. That is the immediate purpose.

Contemporary possibilities of terrorism are especially frightening due to new technologies. Potentially, weapons of mass destruction might be involved. Terror is not simply a function of technology, however. The means are often simple. Motives are usually indirect. Effects are invariably complex.

The terrorist wrecks havoc in order to terrorize those who see or hear about it. He expects to gain more from the symbolic consequences of violence than from its destructive physical effects. The terrorist intends to alter states of mind as well as to change things physically. At the same time, terror is seldom an end in itself. Ultimately, the terrorist aims to influence the prospective behavior of others by affecting their will to act. For this reason, terrorism necessarily represents a politi-

cal act. Political effects are almost always complex. Effective counter terrorism must usually address the politics involved as well as apply physical defense.

Terrorism is neither rare nor new. Thousands of terrorist incidents occur around the world in any given year. It is more frequent than major war, less frequent than other efforts to bring change by peaceful means. There is probably no more of it now than in the past, controlling for growth of societies, but the general public is assuredly more aware of it due in part to advances in international communications. Five hundred years ago, North Americans did not know that there was a Europe, much less that terrorist events occurred within it. Forty years ago, the Viceque Rebellion was almost entirely unknown outside East Timor at the time that it occurred. Today, many terrorist events in far-flung corners of the world are instantly recognized around the globe.

WHAT IS TERRORISM?

Modern usage of the word “terrorism” owes much to the Jacobins during the French Revolution. The Jacobin movement advocated democracy in the form of universal suffrage and also proclaimed very high standards of probity for personal and public conduct. In September 1793, the radical Committee of Public Safety in France under leadership of Robespierre and the Jacobins publicly decreed “terror”, called by that name, against enemies of the Revolution in order to assure the “reign of virtue”. Agents of the Committee murdered, maimed and also seized and destroyed property of alleged enemies for nine months until Robespierre’s arrest and execution. Foreign and domestic critics of Jacobin political objectives and methods, including Britain’s Edmund Burke and conservative continental European governments, fulminated against the French “Reign of Terror”. Critics spoke louder to later generations than did the Jacobins. That period of French history is still commonly identified as “The Reign of Terror”. Perhaps this helps to explain the persistently perjorative connotations associated with the word “terrorism”.

Terrorism is the subject of much recent study and comment. Many book-length treatises and collected works have general import, including Clutterbuck [1], Crenshaw [2], Ford [3], Hoffman [4], Laqueur [5, 6], Long [7], Kegley [8], Rubenstein [9], Schlagheck [10], and Wieviorka [11]. Contemporary theory is also represented within several important essays, including Adkinson, Sandler and Tschirhart [12], Enders and Sandler [13], Hamilton and Hamilton [14], and Merari [15]. A few recent studies systematically examine connections between terrorism and other manifestations of political conflict, including O’Brien [16]. Many additional scholarly monographs, collections and articles speak to specific forms of terrorism or specific instances of it. A few journals devote themselves particularly to the subject, notably including *Terrorism and Political Violence*. Several compendia document recent terrorist events, including several iterations of the data set *International Terrorism: Attributes of Terrorist Events*, which contributes to numerous systematic studies [17]. The *Rand-St. Andrews Chronology of Terrorism*,

also iterated, is another frequently employed compendium [18]. Government reports and individual political commentaries are too numerous to mention.

The term “terrorism” is generally employed today to denote fearful violence inflicted for explicit political purpose. There is disagreement about what else, if anything, to include under the label. Consensus upon a strict definition exists among most scholars who study terrorism consistently over time and space [19]. Governments and public commentators, most of whom attend primarily to a few attention-getting events of the moment, do not necessarily agree. Some seek to excuse some actions that they prefer not to call “terrorism”. Others conflate terrorism done for political purpose with other forms of reprehensible violence without regard to motive or long-term effect. Broad and behaviorally inconsistent definitions are potentially misleading.

It may not be surprising that interested parties in government and the public frequently confound terminology in discussion of terrorism. The label “terrorism” itself has practical consequences. To call another a “terrorist” is to name an outcast, given traditional prejudice against the word. To call a terrorist by another name—perhaps “freedom fighter”—grants superficially greater political and moral legitimacy. Whether or not to attribute an event to terrorism may even affect whether or not insurance policies that exclude acts of terrorism will compensate for losses [20].

It is also not surprising that some interested parties conflate terrorism with other acts of violence. Terrorism is merely one of several forms of violence that threaten ordered societies. Others of these, including simple criminality, may be even more widespread. The physical effects of violence are damaging no matter the cause. It is tempting to clump all bad things together in hope of addressing them all at once.

Conflating terrorism for political purpose with other forms of violence may be seriously misleading. The motives of terrorism, guerrilla warfare, simple criminal violence, and psychopathology are presumably different. The terrorist seeks primarily symbolic political effect. The guerrilla warrior seeks, along with other things, to sap the strength of established security forces by unconventional means. The simple criminal presumably inflicts violence incidentally in pursuit of personal material gain. The psychopath may have no comprehensible reason at all.

In addition, the more broadly is terrorism defined, the less clear it is how to counter it [19]. Counter-insurgency warfare against guerrillas has well-developed doctrine and training. So does criminal justice and peace officer training. Psychiatrists possess their own theory and methods for dealing with irrationally destructive personal behavior, if given the chance. These are different from each other, however and none is sufficient to the special requirements of curbing politically motivated terrorism. The methods that one can and ought to use in response to each are not identical. Martial law and other suspensions of political liberties may be tolerable in the face of guerrilla warfare but are seldom politically or morally acceptable in response to mere terrorism. Counter-threats directed primarily to personal material interest are largely wasted upon the terrorist; he seeks more than

just tribute. On the other hand, appeals to political interest and principle are largely wasted upon both the criminal and the psychopath.

The purpose of this chapter is briefly to elaborate and extend contemporary theory of terrorism in order to facilitate comprehensive discussion of technology within terrorism and counter terrorism. Technical literature abounds, especially relating to particular technologies, and especially relating to especial needs of law enforcement and military defense. Very little has been done since Wilkinson [21] comprehensively and explicitly related technology to terrorism, strictly defined.

For present purposes, the term "terrorism" is defined strictly and in accordance with present scholarly convention. "Terrorism represents a publicized program of episodic violence targeted upon non-combatant persons and property for purpose of affecting political attitudes and behavior". Publicity is essential to terrorism's purposes, even if limited to word of mouth, in order to communicate demands and to signal accomplishments. Terrorism normally involves a succession of destructive events. It is difficult to change attitudes and behavior by means of a single isolated act. At the same time, it is customary to distinguish episodic terrorism from continuous military campaigns, including strategic bombing of civilian targets during World War II and other major wars. Terrorism is further distinguished from guerrilla warfare and conventional military operations that target soldiers and other recognized combatants. Terrorist violence aims ultimately to affect public policy and governance and not necessarily other matters. It aims to do so by changing attitudes and behavior among immediate and secondary witnesses, primarily through intimidation.

Why Terrorism?

Terrorism is by definition a tactic undertaken for strategic political effect. It helps to think like a terrorist in order to comprehend the political context within which the terrorist operates. Politics generally resembles a strategic game whose outcome rests upon interdependent choices among two or more parties. Parties to politics may include individuals, governments, or other organizations, depending upon circumstances. Politics further involves a bargaining process, not necessarily peaceful, in which parties attempt to influence one another's choices [22]. One may seek to induce another to act in ways he did not originally intend. Alternatively, one may seek to deter another from doing what he planned. Various general strategies are available for this purpose, including argumentation (both affirmative and negative), reward, promise, punishment and threat. Several instruments are available to suit each of these strategies.

Terrorism is one of many instruments that may be employed in an attempt to change political behavior by the application of punishment and threat. It is an intermediate technique in the spectrum of violence. It is more destructive than most strikes and other demonstrations, less damaging than most conventional military campaigns. The deadly logic of terrorism relies upon the insight that death and damage inflicted upon non-combatants may demoralize observant citizens and

government officials, undermine support of established leaders, and eventually lead to change of policies or governments. He who resorts to terrorism may also employ other instruments at other times, including conventional military force if he is able. The terrorist presumably employs terrorism because it suits his purpose and is consistent with his abilities.

A terrorist attack constitutes a non-verbal signal intended primarily to convey an intimidating message to particular audiences. Any such act demonstrates ability and willingness to behave destructively. The magnitude of an attack further signals terrorist strength [23]. Apparent strength implies ability to conduct more attacks in future.

A terrorist attack may intend to send a signal to any of several audiences for any of several instrumental purposes. It may be employed in an attempt to demoralize agents of an established government, including the wave of assassinations inflicted upon village leaders within South Vietnam during the late 1950s by opposition groups associated with the Viet Cong. It may be employed in an effort to undermine public support of a government by demonstrating that government's inability to protect its citizens. This is a frequent aim among insurrectionist movements now and in the past. It may be employed abroad in order to discourage foreign support for domestic policies and governments, including Palestinian attacks within Europe from the 1960s onward aimed to coerce change in foreign support of Israel. It may be employed in order to attract new adherents to one's own cause by demonstrating will and capacity for action. This presumably was an important purpose of the Boston Tea Party of 1773. It may be employed in order to reinforce commitment among one's own followers and to forestall decay of organization due to inaction. One suspects that was one reason why the Provisional Irish Republican Army broke so many truce agreements in Northern Ireland during the 1980s. In practice, the signal represented by a terrorist attack may reach several audiences at once and may serve more than one political objective.

Terrorism is not necessarily best for all purposes, however, and some terrorists may wish to employ more powerful instruments instead. Guerilla warfare targeted upon security forces is sometimes an alternative to terrorism targeted upon non-combatants, if one is able to do it [24, 25, 26]. Guerrilla warfare impacts governments directly and may precipitate swift change of policy. The devastating attack upon U.S. Marine barracks in Beirut in 1982 by Islamic militants led to U.S. withdrawal a few months later. The problem with guerilla warfare is that it usually requires more resources, more skill, and more organization than does a mere terrorist campaign. The targets of the guerrilla are at least supposed to be prepared to fight back.

Conventional military force is even more effective for some purposes [27, 28]. Terrorism does not work well to gain and retain control of territory. It may help to undermine existing authority but does not immediately establish new authority, any more than does guerrilla warfare. In order to control territory, the terrorist and the guerrilla are both advised to turn to conventional military force, if they are able to do so [29]. Terrorism is not even the best means for inflicting

maximum physical damage. The physical consequences of a terrorist attack are frequently small, temporary and uncertain compared to what may be achieved by a conventional military operation. Conventional military force, of course, requires even more resources than does guerrilla warfare; many terrorists refrain from it more from weakness than preference.

The terrorist may also wish that he could rely upon less destructive instruments, including peaceful methods of coercion. Terrorism, to the extent that it is physically successful, damages persons and property that the terrorist might prefer to remain intact if he becomes politically successful. Moreover, practice of terrorism frequently prejudices claims of moral legitimacy on behalf of the terrorist's demands for change. Some terrorists resort to terror in sadness as well as anger, convinced that less violent means alone will not produce desired political effects.

Who Are Terrorists?

Individual agents execute most terrorist operations. The individual who pulls the trigger or plants a bomb is not necessarily fully aware of the strategic purpose that directs his actions. The primary terrorist, often behind the scene, is he who purposefully employs and directs individual agents and operations.

Serious terrorists are generally well known. Terrorism is a public activity. It is not and cannot be entirely clandestine. The terrorist may seek to hide the time and place of planned attacks and may also try to obscure the names of his individual agents. The event itself cannot be secret because terrorism must be visible in order to terrorize. The authority and purpose behind terrorist attacks must also be apparent in order to influence attitudes and behavior in desired directions.

Political conditions that give rise to terrorism are also usually obvious and typically involve conspicuous, although controversial, claims of injustice. Most who embrace terrorism do so on the basis of dire expectations. They do not like the way things are and despair of other means to affect the future. Those who see themselves as revolutionaries, leaders of resistance, or guardians of declining order are especially likely to resort to terror. It is a conscionable instrument among some who are dispossessed, disadvantaged, or downtrodden [30]. It is also occasionally appealing as a last resort to beleaguered authorities that are desperate to extend or hold onto power.

Terrorists are comparatively weak in most cases and often embrace terrorism because they are not strong enough to do things differently. They are able to inflict episodic damage but are usually deficient in constructive power and compelling authority [31]. Dominant parties associated with the established order may rest upon their laurels. The wealthy may buy change. Powerful authorities may be able to sustain conventional military campaigns. Those known to be strong may get their way merely by threatening military action. The terrorist often resorts to terror because he is unable to employ effective alternatives. Terrorist tactics are comparatively easy to execute and involve comparatively small risks if one has little to lose from retaliation.

Terrorists are not new. Nor do they always serve unworthy purposes. Jewish Zealots employed terror in an effort to resist Roman policies within Jerusalem and other parts of Palestine two thousand years ago. Terrorism erupted after Roman edict of direct taxation at the beginning of the present era and persisted at least until the fall of Masada decades later. The American Revolution began with terrorism, including the destructive but not lethal Boston Tea Party of 1773. Ethan Allen and the fabled "Green Mountain Boys" behaved as little more than terrorists during their 1775 rampage across New York and southern Canada although they occasionally also attacked lightly defended British military installations. The modern state of Israel grew out of terrorism. The Irgun and other Jewish groups violently resisted British administration of Palestine before and after World War II, including attacks upon property and persons that served or supported British authority. Some Arab Palestinian groups did similarly at the same time. Growing strength allowed Jewish nationalists to develop also conventional military units by 1948; these were subsequently incorporated within the Israeli Defense Force after independence.

Many well-known parties employ terrorism today and did so in the recent past. Notable recent terrorists include agents for numerous non-governmental organizations. Among these are: various Palestinian entities such as the Popular Front for the Liberation of Palestine and Al Fatah; the Kurdish Workers' Party within Turkey and Iraq; Sikh nationalist organizations within the Punjab and other parts of India; and the Provisional Irish Republican Army acting within Northern Ireland and England. No short list can do justice to the whole. Various "watch lists" distributed by the Federal Bureau of Investigation and other U.S. intelligence agencies identify thousands of political organizations connected to terrorism today and denote hundreds that deserve constant attention.

Some terrorism is popularly attributed to particular individuals. Osama bin Ladin, an exiled Saudi who took refuge in Afghanistan, is frequently mentioned in this regard. Strictly personal terrorism is uncommon, however. It is difficult to sustain a program without durable organization. It is difficult to effect important political change if others interpret violence merely as personal vendetta. Effective terrorist leaders typically portray themselves as representatives of conspicuous groups and movements. Usually they are.

Some governments also contribute to terrorism, although more sponsor it indirectly than employ it directly. Most refrain from conspicuous involvement in terrorism, either because they have no need for it, do not approve of its methods, or fear retaliation. Governments that employ terrorism directly and conspicuously are often comparatively weak and insecure. A few employ terror against their own peoples in effort to consolidate power, as did France's Committee of Public Safety in the 1790s. Others terrorize their own in an effort to forestall collapse, as did the government of Mohammed Reza Shah Pahlavi in Iran prior to its downfall in 1979. Some employ terror against hostile neighbors or other foes for ostensibly defensive purposes. Modern Israel since 1948 has periodically attacked non-combatants within Jordan, Lebanon and elsewhere. A few others occasionally

employ terrorism for blatantly coercive purposes, including Libya within Chad during the 1970s and 1980s.

COUNTER TERRORISM

Counter terrorism attempts to negate terrorism. Of necessity, it is as old as terrorism itself. Governments and other established authorities threatened by terrorism have each relied upon it for thousands of years. Many have cooperated with one another for this purpose. The international community as a whole took notice at least as early as 1934 when the League of Nations established the Committee for the International Repression of Terrorism.

Counter terrorism resembles terrorism in a few respects. Both involve programs of action and not merely singular acts. Both counter terrorism and terrorism depend upon political influence, not merely physical prowess. In order to fully prevent terrorism one usually has to influence the terrorist to choose to stop. Both usually require institutional organization, perhaps counter terrorism even more than terrorism. Effective counter terrorism typically requires large social investments and political programs beyond the reach of most small groups. In many cases, only strong governments are empowered to do counter terrorism well.

In some other respects, counter terrorism represents the opposite of terrorism, including who is most likely to undertake a serious counter-terrorist program. While anyone who fears to be a target may worry about terrorism, those with most to lose are most likely to do something about it. Thus counter terrorism is usually associated with those privileged to take comfort in the present social and political order. The counter-terrorist typically represents the established order of monetary wealth, property, political power and policy within and among societies. This is opposite to the typical terrorist distressed and dissatisfied by the present state of order.

The tactical and political objectives of counter terrorism are also opposite to terrorism. The tasks of counter terrorism typically emphasize defense, not attack, and deterrence, not inducement. Defense in this context involves protection of specific persons and property in order to defeat a terrorist operation underway. This usually includes physical security, either passive or active, connected to specific sites. The focus of concern is the terrorist agent and the weapons in his hands. Physical security alone is usually insufficient unless protective devices provide broad shields, are omnipresent, and perfect. The terrorist has many potential weapons from which to choose, many potential targets from which to select, and many ways to get around incomplete defenses.

Deterrence aims to dissuade the terrorist from commencing an attack [32]. Assuming that a terrorist resorts to violence deliberately as a means to a political end, and assuming that defense is uncertain, it makes sense to try to influence the terrorist either to abandon his political objectives or choose less destructive methods. Deterrence does not necessarily require physical action by the counter-

terrorist although it often includes such. The primary focus of concern for deterrence is the primary terrorist who directs agents for a purpose.

Counter terrorism occasionally includes pre-emptive attacks upon known terrorist bases, usually for purpose of deterrence. Such operations rarely expect to eradicate terrorist capabilities, something virtually impossible to accomplish against dispersed and easy-to-replace agents and weaponry. Attacks upon terrorists usually aim merely to punish and by punishment to deter future terrorist operations.

An important question to answer before devising any counter-terrorist strategy is whether one objects more to terrorists' methods or to terrorists' political objectives. If one particularly deplores violence, one way to limit it is to accommodate all or part of terrorists' demands. Appeasement works, up to a point, despite a bad name earned following the Munich Conference of 1938, provided that one is willing to accept the ultimate political results. If, on the other hand, one objects most to the substance of terrorist demands, some terrorism may be an acceptable price to pay for standing up for one's own political principles.

Another question is to what extent to rely upon defense and to what extent upon deterrence. Strong defense against terrorism does not necessarily imply effective deterrence, nor vice versa. Defense against terrorism is almost invariably probabilistic. Some defenses may protect some sites some of the time. Few known defenses are sufficient to protect all potential targets against all potential weapons. Further, most terrorists know that it is not necessary to succeed in every instance in order to inflict terror overall. Terrorists, therefore, are generally motivated to keep trying if at first they don't succeed; and they probably will succeed eventually. At the same time, deterrence is seldom perfect either, and leaves no immediate protection when it fails.

Counter-terrorist defense is complicated by problems related to the offensive-defensive balance. The marginal social cost of deploying and maintaining counter-terrorist devices and procedures often exceeds the cost to terrorists to overcome those same defenses. The price of full spectrum defense may exceed the expected value of objective losses likely to be halted. Partly for this reason, counter-terrorist defense is customarily selective. Wise effort assesses the likelihood of various terrorist possibilities before committing large sums to uncertain defense.

Deterrence of terrorism is also complicated. The object of deterrence is to dissuade another party from doing what he intends. This requires a clear and consistent signal regarding what another ought not to do. Generally, the more broadly deterrence is aimed, the more diffuse is the signal. Diffuse signals are usually less effective. Unfortunately, assuming that another party has many alternatives from which to choose, selective deterrence may prevent one bad outcome but fail to prevent other undesirable results. Reliance upon deterrence is thus doubly risky: deterrence may fail outright; or deterrence may succeed narrowly but undeterred alternatives prove unfortunate, too [33].

Selective deterrence involves difficult choices regarding what to deter and what to tolerate. Some sorts of violence may be judged most needful to prevent, including against certain targets using certain awful weapons. Assuming that the terrorist's will to do violence may find an outlet somewhere, it may be necessary to leave some targets at risk in order more effectively to deter attacks upon targets that one worries most about. Worse yet, as Enders and Sandler [34] report upon basis of systematic study of terrorist events, terrorist's alternatives are demonstrably substitutable: improvement in deterring one type of terrorist attack is associated with increased likelihood of other forms of attack.

Another issue in deterrent strategy concerns where to concentrate influence within the terror process. One may try to persuade a potential terrorist that his political aims are unworthy or lie beyond reach by any means. One may try to undermine confidence in ability to do damage. One may attempt to convince a potential terrorist that he cannot gain specific benefit from damage as he admittedly can inflict. Or one may seek to assure a potential terrorist that his destructive acts will result in unacceptable retaliation [35]. The ultimate objective remains the same at each step of the process: to influence would-be terrorists to refrain from terrorism. Methods of imparting influence differ, however.

In sum, counter terrorism is generally more difficult to accomplish than to arrest mere criminal violence. For one thing, the criminal seldom chooses targets indiscriminately. He usually attacks where money is. Sadly, even sophisticated counter-terrorist strategy may not suffice to prevent destruction owed to seemingly irrational personal impulses, including bombing of the U.S. Federal Building in Oklahoma City in 1995 by Timothy McVeigh, and violence inflicted by the "Unabomber," Theodore Kaczynski.

TECHNOLOGY AND TERRORISM

Technology shapes terrorist events. Terrorism is initiated for political reasons and political consequences are ultimately paramount. Nevertheless, the political path from start to finish is restricted by available technologies. Many recent and sophisticated technical advances enhance horrible possibilities of terrorism, including advanced munitions, energy devices, chemical, biological, radiological, or cyber-weapons. Some of these potentially could do extraordinary harm whether employed as weapons of mass destruction or as weapons of mass disruption to disarray the infrastructure of a society [36]. The danger of immediate superterrorism based upon such new technologies is real but improbable compared to the virtual certainty that ordinary terrorism will persist [37]. The substratum of widely installed technologies guides ordinary terrorism most of the time. The terrorist, by and large, is more imitative and habitual than technically imaginative [38, 39]. To this day, most death and destruction due to terrorism results from knives, guns and simple bombs. The savvy terrorist and the prudent counter-terrorist both recognize ordinary technologies that determine what is practical for

each. Readily available technologies have improved with time although they usually lag behind the latest laboratory developments. A contemporary terrorist is able to do things that his predecessors found impractical or did not imagine.

Technology ordinarily relates to terrorism in at least three ways, all of which have changed over time: 1) Weapons technology produces implements that terrorists may use. 2) Transportation technology limits the speed, distance and magnitude of terrorist operations. 3) Communications technology also governs the speed and distance of political effects.

1) The terrorist usually employs readily available and easily controlled weapons. By and large, he adopts new weapons technologies belatedly, after military, commercial and sometimes even criminal uses are established. The terrorist prefers simple and familiar weapons for several reasons. They are often readily available. Most are comparatively inexpensive. Less complexity predicts greater reliability. Often used weapons are frequently small, portable, easy to hide before the event, disposable, do not require great skill among agents to prepare or use, and have long records of accomplishment.

For centuries, most terrorists relied primarily upon the knife. Zealots used knives to kill prominent citizens at public gatherings in Jerusalem and other cities. The knife remained the preferred implement of terrorism until the 19th Century. Guns existed long before most terrorists began to use them. Guns appeared occasionally during the American Revolution and the 1790s Reign of Terror in post-revolutionary France but were not commonly used in terrorists' hands until a half-century later. Rapid-fire hand weapons date from the late 19th Century but were not commonly employed for terrorism until well into the 20th Century. Indeed, some devices such as the sub-machine were used for criminal purposes even before many terrorists adopted them. Fully automatic weapons did not become frequent tools of terror until the 1960s or later, depending upon locality. Now, of course, fully automatic rifles and handguns are widely employed.

The story of explosives follows a similar course. The gunpowder bomb is as old or older than the gun itself, was used for military purposes from the beginning, but did not find much employment among terrorists until the 18th Century. Most subsequent developments in explosives were also long known before finding use in terrorism. Nitroglycerin, picric acid and combustible derivatives of petroleum were commonly available before Anarchists employed them across Europe in the late 19th Century. Dynamite was invented by Alfred Nobel in 1866, quickly found both military and commercial applications, and eventually appeared as a frequent terrorist weapon at the beginning of the 20th Century. Other high explosives, including trinitrotoluene (TNT) followed with similar delays. Most recently, plastic explosives have belatedly appeared in terrorist use. To this day, however, many important terrorist bombings rely upon old-fashioned technologies, including the so-called "fertilizer bomb".

Poisonous and infectious chemical-biological-radiological (C.B.R.) agents developed as military weapons during the 20th Century also have terrorist potential but are seldom used for this purpose. Some chemical weapons have been em-

ployed on battlefields from World War I to the Persian Gulf War of the 1980s. A few chemical agents are widely available. None is ordinarily used in deliberate attacks upon civilian targets for purpose of inflicting terror. Attacks such as undertaken by Aum Shinrikyo (Sacred Truth) using sarin nerve gas within a Tokyo subway in 1995 are very rare. Most C.B.R. agents have technical disadvantages as weapons for any use, including terrorism: most are difficult to transport; many have uncertain reliability; and nearly all are difficult to control in use.

Some governments also routinely equip military forces with deadly and far-reaching weapons systems capable of instilling terror by bombing or bombarding civilian targets. So far, most governments refrain from using such weapons except in conjunction with major military campaigns. Threats of nuclear attack upon cities, the basis for contemporary nuclear deterrence, are especially horrifying. Nuclear weapons, although now available in several forms to several governments, have not ever been employed since Hiroshima and Nagasaki at end of World War II. Conventional munitions delivered by tanks, long-range artillery, bomber and fighter-bomber aircraft, sub-sonic and ballistic missiles are also frightening. Civilians sometimes suffer incidental damage from such military weapons aimed primarily at combatants. Sometimes civilian damage appears to be more than incidental. Nonetheless, governments seldom admit to deliberate invocation of terror except in wartime, and not always even then. Most have too much to lose from retaliation in kind.

2) Technology of transport also makes a difference. Historically, terrorism is mostly local. Terrorist agents traditionally strike close to home although, increasingly, some also undertake operations far away. Advances in the speed of personal transportation facilitate extended reach of terrorism. In principle, a contemporary terrorist agent could travel to a target thousands of miles away in less than a day, complete his mission, and return at similar speed. Some do. This has become possible only recently. From earliest civilization until little more than 200 years ago the speed of long distance transport was generally limited to no more than four miles per hour. Men on foot or horses normally go no faster than this, nor did most sailing ships until the late 18th Century. The pace of transport in some parts of the world increased by an order of magnitude during the 19th Century with introduction of railroads and fast steamships. Automobiles and trucks built upon the internal combustion engine, introduced in the 20th Century, helped to reach places not served by railroads. The airplane, also introduced in the 20th Century, increased maximum speed of personal transport by another order of magnitude. At the beginning of the 21st Century a terrorist agent relying upon commercial and/or general jet aviation can travel between major cities around the world hundreds of times faster than his 18th Century predecessors. One cannot reach all points of the globe so rapidly. Some locations, including many rural areas of the world, remain beyond the immediate reach of recent technologies.

Ease of moving weapons has not necessarily kept pace with improvement of personal transport. Terrorists traveling by commercial air must usually rely upon weapons cached or found at or near the scene. Personal weapons and other light

arms are otherwise mobile but usually move at land- or sea-speed when carried over appreciable distances. Long-range transport of heavy weapons is and always has been difficult except for the military forces of a few countries. These technological limitations restrict terrorists' choice of weapons and reinforce tendency to rely upon small arms and locally available explosives.

3) Communications technology is also significant to both tactical and strategic aspects of terrorism. Tactical communications between the terrorist and his agents, as well as communications among agents if there is more than one, are necessary to execute most effective attacks. Strategic communications, both verbal and non-verbal, are essential to the political purposes of terrorism. The terrorist must signal responsible parties what he demands as condition for ending terrorism. Violent actions must be reported beyond the immediate scene if terror is to spread. The terrorist needs also to signal his accomplishments to present and prospective supporters in order to maintain and build his organization. Verbal communication is not necessarily required in every instance and at every step of the way provided that sufficient ground is previously established to be confident that non-verbal signals will be interpreted as one desires. For example, the terrorist does not necessarily announce a public claim of responsibility for each and every atrocity he commits [40]. Some form of communication, verbal or non-verbal, is always essential, nonetheless.

Advances in communications technology have enabled more complex and more far-reaching terrorist campaigns than previously practical. In some instances, technology now permits orchestrated terrorism where previously it was impossible.

In 1840-41, small units under U.S. Navy Lt. Charles Wilkes, commander of the United States Exploring Expedition repeatedly attacked and destroyed villages in the Pacific, including Fiji, Samoa, and Drummond Island in the Gilberts. Superficially and in hindsight this might appear to constitute a conscious campaign of political terror directed by the U.S. government. It was not and could not be. Communications technology of that day permitted no quick means to communicate with ships at sea and Wilkes remained entirely out of touch with Washington most of this time. The U.S. Exploring Expedition set out in 1838 to investigate the rumored existence of Antarctica and returned in 1842 after also surveying the North American coast and visiting various unfamiliar places in the Pacific. The Secretary of the Navy initially directed the expedition, when in contact with native populations, "to appeal to their good will rather than to their fears." Ensuing violence reflected mostly personal motives, including efforts to bring alleged cannibals to justice and reprisal for theft and injury inflicted upon members of the expedition who, among other things, seized artifacts that later became the foundation of the Smithsonian Institution collection. Wilkes was belatedly brought to court-marshal for exceeding instructions after return of the expedition in 1842 and after men under his command reported what had been done. He was eventually acquitted of all charges relating to mistreatment of civilians and retained his commission.

Critical dimensions of communications technology affecting terrorism include the range, speed, and carrying capacity of signals transmitted via particular media. Dramatic advances in communications technology over the past century and a half permit the terrorist to convey messages further, faster, and with more content than before. As is true of weapons and transportation, installed technologies matter most. The terrorist usually relies upon widely available communications media.

Until the 1840s, with few exceptions, no message traveled faster or further than the pace and range of human transport. In effect, nearly all communications, including tactical communications, signals of terrorist demands and news of terrorist attacks, used to be limited to word of mouth and hand-carried paper. Exceptions generally had limited applications. The "ancient telegraph"—smoke-signals relayed from hilltop to hilltop—known at least as long ago as 5th Century B.C. Greece, conveyed little information, worked only in presence of appropriate hilltops, and only for those who controlled the hilltops, which terrorists seldom did. Pigeons and other trained birds occasionally were employed for centuries to carry bits of information, including first news to London of Wellington's victory at the Battle of Waterloo in 1815, but also saw limited use for obvious reasons relating to reliable range and carrying capacity.

The bulk of information still travels at human pace, although that pace is faster now than it once was. Some new technologies have increased carrying capacity of long-distance communications without breaking the human speed barrier. Printed media, including books, magazines, and newspapers, as well as ephemeral publications such as newsletters, are more numerous due in part to computer-assisted design and production. As a result, more is put to print than previously and the terrorist has more opportunities to make known his demands and accomplishments, provided that his intended audience identifies his signal within the burgeoning noise of numerous other messages.

Other technologies newly available in the late 20th Century provide additional channels to transmit large amounts of information, including audio, video, and data tape, plus parallel disk media. The Iranian revolutionary movement inspired by the Ayatollah Khomeini that toppled the Shah in 1979 relied in part upon audio cassette tapes dispatched from Paris in order to direct agents and other followers within Iran.

The velocity of some communications increased significantly in the latter half of the 19th Century. Invention of the telegraph in 1844 provided the first reliable means to send signals more rapidly than human transport over long distances. Bandwidth was limited. Messages could travel fast only where wires existed and these initially followed railroad lines. Telegraphy across large bodies of water was enabled only decades later. The telephone, introduced in the late 1870s, improved upon the telegraph in some respects, including ability to carry more information, but was also limited at first to land-wires. The radio-telegraph, invented in 1895, reduced dependence upon installed wiring but was initially limited to use between designated facilities, including, for the first time, instantaneous communication

with some ships at sea. These technologies at first conferred more tactical benefit upon governmental counter terrorism than upon insurgent terrorism. 19th Century terrorists, by and large, did not control these media. Terrorists gained some benefit in spreading terror from early use of telegraphy and telephony among some urban newspapers that used these new devices to acquire information more rapidly than before. Once in print, however, newspapers reached the public little more rapidly than before.

Broadcast technology introduced in the 20th Century expanded the scope of rapid communications but initially remained outside direct control of most terrorists. Commercial radio and, more recently, television permit the terrorist to convey political messages rapidly to distant audiences, provided that he can cause the broadcaster to transmit his message. The graphic content of television is particularly helpful to spread terror if one can exploit it.

Today's internet connections among computers and telephonic facsimile transmission provide additional high-speed channels to transmit both words and images. The rapidly growing internet facilitates several forms of instantaneous and far-reaching communication, including point-to-point transmission via electronic mail and largely self-regulated global broadcasting via the World Wide Web. Some contemporary terrorists employ the internet for these reasons. "Fax" transmission is not necessarily so versatile but also finds use for some point-to-point terrorist communications.

Terrorists generally rely upon publicly available technology for communication just as they do with regard to weapons and transport. In principle, public access to fast moving and content-rich communication is now available through several channels throughout most of the world. In practice, the effective speed, range and carrying capacity of public communications varies greatly for different purposes and from place to place. Telephone and e-mail are more or less instantaneous and are widely available but do not provide satisfactorily secure media for tactical messages to and among terrorist agents. For political purposes, including dissemination of reports of terrorist attacks, most terrorist signals still follow circuitous paths through multiple media before reaching all of their intended audiences, including transmission and retransmission via radio, television, and newspapers. Nor do advanced communications presently extend to all localities, especially not to rural areas within developing societies. It is not accidental that terrorist attacks appear to congregate within and near major cities today. Not merely do cities include many inviting targets; reports of violence spreads further and faster out of major cities that are directly connected to global communications networks.

Interconnected urban mass media are especially important to the contemporary terrorist. For political purposes, the terrorist now depends greatly upon the journalist to help convey his signals. This does not imply that journalists necessarily subscribe directly to terrorists' purposes. It is, and generally recognized as a symbiotic relationship [41]. Journalists report "news". "News", according to a widespread bias within modern journalism, necessarily includes threats of political violence and, especially, violent political events themselves. The terrorist makes

“news”, partly but not merely in order to stimulate journalistic reports of what he wants and what he has done. Images and words emanating from an observant reporter may reverberate widely once transmitted and re-transmitted among radio stations, television stations, newspapers and other mass media, many of which pluck “news” from one another as well as from their own proprietary reporters. The web work of modern journalism penetrates more corners of the globe today than in the past. It now extends among most major cities of the world although it does not necessarily extend everywhere into the countryside. It is now practical in some cases for a terrorist to attack close to home, confident that word will get out, in order to terrorize far away; or vice versa. This is the most important meaning of the current catch phrase “global terrorism”.

COUNTER TERRORISM AND TECHNOLOGY

Counter terrorism depends upon technology in order to deter as well as to defend against terrorism. The counter-terrorist benefits from many advances in technology, sometimes more quickly than the terrorist. Some governments may be able to mobilize new devices and procedures not yet generally available for public use. Generally speaking, however, most successful counter-terrorist strategies rely primarily upon widely disseminated technologies. This applies similarly to weapons, transport and communications.

Effective counter terrorism faces a broader challenge than does terrorism. The terrorist may choose where, when and how to attack. The counter-terrorist must prepare to defend any likely target at times and by means of the terrorist’s choosing without knowing in advance what the terrorist will choose. He must try to deter many possible actions, not merely one. Ideally, counter terrorism is omnipresent because there are many potential terrorists to deter and many potential targets to defend. This is practically impossible, if only because it is too costly to achieve. Focused effort and widely available methods are at least as valuable to the counter-terrorist as the terrorist.

Technical requirements of defense and deterrence are not necessarily identical. For purpose of defense, the counter-terrorist wants to stop the terrorist from completing destructive operations. The first line of defense is to eradicate or incarcerate all prospective terrorists. This is more easily said than done in any morally or socially acceptable way. The second line of defense is to deny to terrorist agents access to things that they need to do their deeds, including weapons, transport, and tactical communications. It is sometimes possible, within limits, for governments to deny access to some advanced technologies that are not yet available for public use. Secrecy and physical security are the primary instruments for this purpose. The United States government and most other nuclear powers treat information relating to nuclear weapons technology as restricted data and prohibit dissemination. Advanced military weaponry, transport and communications devices are usually stored under heavy guard. It is more difficult to deny access to publicly avail-

able weapons or other technologies although magnetic security gates and other familiar second line defenses are deployed for precisely this purpose. The third line of defense is to arrest a terrorist operation at the scene, hopefully before destruction is fully unleashed. This necessarily involves physical security. Many devices, new and old, are potentially helpful. The challenge of physical security includes more than merely to invent appropriate techniques. It is also to deploy the right devices at the right place at the right time, along with personnel to employ them, properly trained in their use. Advanced defense technologies that are not ordinarily widely distributed are especially difficult to deploy in timely fashion.

The technical requirements of deterrence depend in part upon what strategy of counter terrorism one pursues. Many deterrent strategies require more than mere technical proficiency and depend also upon propaganda, diplomatic skill, and expenditures for other than defense. In order to convince terrorists to abandon their objectives as hopeless or to persuade them that they cannot gain specific benefit from terrorism, one must usually invest in nation-building in order to reinforce the solidity of established order. Extended deterrence of terrorism aimed at change abroad may require foreign aid to assist nation-building within vulnerable societies. Technical requirements for undermining terrorists' confidence in ability to inflict damage are similar to those required for effective defense. The additional requirement for this purpose is to publicize the efficacy of those defenses. Unfortunately, publicity may assist the terrorist to identify ways to avoid existing defenses. As a result, the counter-terrorist sometimes knowingly weakens defense in effort to strengthen deterrence. Technical requirements for a strategy of retaliation against terrorists and terrorist agents are at least as onerous as those required in counter-insurgency warfare against guerrillas. This includes capability to inflict terror upon terrorists. This is sometimes technically more difficult than to terrorize guerrilla warriors whose more elaborate infrastructure may be easier to locate and to damage.

An important challenge in devising any counter-terrorist strategy is to anticipate probable events. It helps to identify who are likely terrorists. This is an intelligence task. Most good estimates depend as much or more upon open sources of information available to the public as they do upon advanced intelligence technologies. It also helps to anticipate likely targets and likely techniques of terrorism. This is also in part an intelligence task. Success depends in part upon adequate specification of intelligence requirements in advance. Unguided, even the best intelligence sources and the most sophisticated intelligence methods presently available, including signals intelligence, are unlikely to provide timely warning of all impending terrorist attacks. As noted previously, contemporary terrorists usually select conspicuous targets whose damage or destruction is likely to attract journalistic attention. In addition, terrorists generally rely upon widely available weaponry, transport and communications. While it may be prudent to investigate techniques for dealing with possible but improbable super-terrorism based upon new technologies, this is not enough [42]. One wants also to find better ways to

deal with ordinary terrorism, remembering that even ordinary terrorism is usually more difficult to control than simple criminality.

SUMMARY

Terrorism represents a program of political action by violent means. It deliberately inflicts damage upon non-combatant persons and property. Its immediate purpose is to induce fear among those who witness the events. It ultimately aims to alter prospective political behavior among immediate witnesses and other parties. Terrorism differs from superficially similar damage inflicted for other reasons, including criminal violence in pursuit of material gain.

Terrorism is an ancient political instrument used mainly by parties who are aggrieved by the present political and social order. The issues are usually obvious and customarily include claims of injustice. The terrorist's methods may always be unworthy. His ultimate objectives are sometimes admirable. Terrorism is especially appealing to those who think that they have much to gain and little to lose. Terrorists customarily represent political organizations that are more capable than most individuals to sustain a campaign of terror. At the same time, terrorist organizations ordinarily lack sufficient power to succeed without violence and are also usually too weak to employ conventional military force.

Terrorism involves non-verbal as well as verbal signaling. The bomb-blast, the bullet and worse are recognizable symbols of punishment and threat if conspicuously coupled to demands for political change. The terrorist depends as much upon his ability to communicate demands and spread report of his deeds as he does upon ability to inflict physical harm. Recent advances in international communications help to spread the terrorist's messages widely and quickly. This may lend the appearance that terrorism is more common today than in the past but that appearance may be deceiving. The world as a whole is certainly more aware of terrorism now.

The terrorist's political objectives, as well his immediate tactics, depend upon installed technologies, including weapons, transport and communications. Generally speaking, the terrorist relies mostly upon simple and widely available methods.

Counter terrorism seeks to negate terrorism. It, too, requires political strategy. It is usually desirable to deter as well as to defend against terrorist attacks. In order to do both these things well one must anticipate likely terrorism because it is practically impossible to deter all potential terrorists and to defend all possible targets against all possible forms of attack. Effective counter terrorism, therefore, distinguishes that which is likely from that which is merely possible. Savvy estimation along this line combines both political and technical analysis. Wise technical investments in counter terrorism also address likely sources, forms, and targets of attack as well as help to prepare against the newest but improbable dangers.

REFERENCES

1. R Clutterbuck. *Terrorism in an Unstable World*. London: Routledge, 1994.
2. M Crenshaw, ed. *Terrorism in Context*. University Park, PA: The Pennsylvania State University Press, 1995.
3. FL Ford. *Political Murder: From Tyrannicide to Terrorism*. Cambridge, MA: Harvard University Press, 1985.
4. B Hoffman. *Inside Terrorism*. New York: Columbia University Press, 1998.
5. W Laqueur. *The Age of Terrorism*. Boston: Little, Brown, 1987.
6. W Laqueur. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. New York: Oxford University Press, 1999.
7. DE Long. *The Anatomy of Terror*. New York: Free Press, 1990.
8. CW Kegley, ed. *International Terrorism*. New York: St. Martin's, 1990.
9. RE Rubenstein. *Alchemists of Revolution: Terrorism in the Modern World*. New York: Basic Books, 1987.
10. DM Schlagheck. *International Terrorism: An Introduction to the Concepts and Actors*. Lexington, MA: Lexington Books, 1988.
11. M Wieviorka. *The Making of Terrorism*. translated by David Gordon White. Chicago: The University of Chicago Press, 1993.
12. SE Adkinson, T Sandler, J Tschirhart. 1987. *Terrorism in a Bargaining Framework*. *Journal of Law and Economics* 30: 1-21, 1987.
13. W Enders, and T Sandler. *Terrorism: Theory and Application*. In: K Hartley T Sandler eds. *Handbook of Defense Economics*. Amsterdam: Elsevier, 1995, 1, pp 213-249.
14. LC Hamilton, JD. Hamilton. *The Dynamics of Terrorism*. *International Studies Quarterly* 27: 39-54, 1983.
15. A Merari. *Terrorism as a Strategy of Insurgency*. *Terrorism and Political Violence* 5 (#4, Winter): 213-251, 1993.
16. SP O'Brien. *Foreign Policy Crises and the Resort to Terrorism*. *Journal of Conflict Resolution* 40: 320-335, 1996.
17. W Enders, T Sandler. *Transnational Terrorism in the Post-Cold War Era*. *International Studies Quarterly* 43: 145-167, 1999.

18. B Hoffman, DK Hoffman. The Rand-St. Andrews Chronology of International Terrorist Incidents, 1995. *Terrorism and Political Violence* 8 (#3, Autumn): 87-127, 1996.
19. AP Schmid. The Response Problem as a Definition Problem. *Terrorism and Political Violence* 4 (#4, Winter): 7-13, 1992.
20. VT LeVine. The Logomachy of Terrorism: On the Political Uses and Abuses of Definition. *Terrorism and Political Violence* 7 (#4, Winter): 45-59, 1995.
21. P Wilkinson, ed. *Technology and Terrorism*. Special Issue of *Terrorism and Political Violence* 5 (#2, Summer): 1-150, 1993.
22. TC Schelling. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.
23. PB Overgaard. The Scale of Terrorist Attacks as a Signal of Resources. *Journal of Conflict Resolution* 38: 452-478, 1994.
24. R Clutterbuck. *Terrorism and Guerrilla Warfare: Forecasts and Remedies*. London: Routledge, 1990.
25. E Guevara. *Guerrilla Warfare*, trans. Brian A. Loveman and Thomas M. Davis. Lincoln, NE: University of Nebraska Press, 1985.
26. VN Giap. *The Military Art of People's War*, ed. Russell Stetler. New York: Monthly Review Press, 1970.
27. HK Tillema. *International Armed Conflict Since 1945*. Boulder, CO: Westview Press, 1991.
28. HK Tillema. *Appeal to Force*. New York: T. Y. Crowell, 1973.
29. T-T Mao. *Selected Military Writings*. Peking: Foreign Languages Press, 1966.
30. G Sorell. *Reflections on Violence*. Translated by T. E. Hulme and J. Roth. Glencoe, IL: Free Press, 1950.
31. KE Boulding. *Three Faces of Power*. Beverly Hills, CA: Sage, 1989.
32. PM Morgan. *Deterrence*. 2nd ed. Beverly Hills, CA: Sage, 1983.
33. T Sandler, HE Lapan. The Calculus of Dissent: An Analysis of Terrorists' Choice of Targets. *Synthese* 76: 245-261, 1988.
34. W Enders, T Sandler. The Effectiveness of Antiterrorism Policies: A Vector-Autoregression-Intervention Analysis. *American Political Science Review* 87: 829-844, 1993.

35. B Brophy-Baermann, and JAC Conybeare. Retaliating against Terrorism: Rational Expectations and the Optimality of Rules versus Discretion. *American Journal of Political Science* 38: 196-210, 1994.
36. RJ Bunker. Weapons of Disruption and Terrorism. *Terrorism and Political Violence* 12 (#1, Spring): 37-46, 2000.
37. M Taylor, J Horgan, eds. The Future of Terrorism. Special Issue of *Terrorism and Political Violence* 11 (#4, Winter): 1-230, 1999.
38. B Hoffman. Terrorist Targeting: Tactics, Trends and Potentialities. *Terrorism and Political Violence* 5 (#2, Summer): 12-29, 1993.
39. MA Wilson. Toward a Model of Terrorist Behavior in Hostage-Taking Incidents. *Journal of Conflict Resolution* 44: 403-424, 2000.
40. DC Rapoport. To Claim or not to Claim: That is the Question—Always! *Terrorism and Political Violence* 9 (#1, Spring): 11-17, 1997.
41. P Wilkinson. The Media and Terrorism: A Reassessment. *Terrorism and Political Violence* 9 (#2, Summer): 51-64, 1997.
42. B Hoffman. Responding to Terrorism Across the Technological Spectrum. *Terrorism and Political Violence* 6 (#3, Autumn): 366-390, 1994.

3

The Group Psychology of Terrorism

Michael A. Diamond

University of Missouri, Columbia, Missouri

INTRODUCTION

Between thirty and forty major armed conflicts take place around the world at any given instant¹. Since 1986 the number of skirmishes has remained constant according to Volkan in his book *Bloodlines: From Ethnic Pride to Ethnic Terrorism* (1997) [1]. Yet, despite the number of battles holding constant, Volkan observes that ethnic and religious terrorism is on the rise. “More terrorist attacks are now carried out by ethnically and religiously inspired groups than by secular groups or individuals. In 1996 the U.S. State Department reported that attacks carried out by individuals and groups have overshadowed state-sponsored terrorism supported by nations....”

During the past decade, hundreds of thousands of people died in ethnic and related “large-group” conflicts. According to the Stockholm International Peace Research Institute (SIPRI), sixty-five thousand people died in the former Yugoslavia – fifty-five thousand in Bosnia-Herzegovina and ten thousand in Croatia – since the commencement of armed conflicts there in 1991.

Afghanistan, Algeria, Angola, Azerbaijan, Bangladesh, Burundi, Cambodia, Colombia, Georgia, Guatemala, India, Indonesia, Iran, Iraq, Israel, Liberia, Myanmar (Burma), Peru, Philippines, Rwanda, Somalia, Sri Lanka, Sudan, Tajikistan, Turkey, N. Ireland, and Zaire have claimed hundreds of thousands more lives. Many of these conflicts have taken place within the boundaries of a single

¹ According to the statistics of the Stockholm International Peace Research Institute (SIPRI) in Sweden and the Conflict Resolution Program of the Carter Center in Atlanta.

country. Hence, they are considered ethnic, religious, and cultural large-group identity-related conflicts, not national conflicts between sovereign countries.”

We begin this chapter with the premise that fewer acts of terrorism today are confined to state sponsorship and that, increasingly, acts of terrorism are rooted in ethnic, religious, cultural and nationalistic, large-group identities. In addition, with the combined ambiguity and vulnerability of nation-state boundaries and affiliations in a global world economy, comprehending the reasons and motives behind violent large-group membership becomes crucial to resolving inter-group conflicts, and ethnic and religious tensions worldwide.

THE CHANGING FACE OF TERRORISM

The face of terrorism is changing. Today, terrorism is associated with public acts of violence and mass destruction, dramatic public performances intended to shock bystanders and symbolize a war between good and evil. The timeliness and relevance of understanding the psychology of large ethnic, religious, nationalistic and cultural large-group conflicts is unmistakable.

According to Crenshaw [2], the “new” terrorists “seek nothing less than to transform the world. Motivated by religious imperatives, they are feared by many observers and bystanders to lack an earthly constituency and thus feel accountable only to a deity or some transcendental or mystical idea.” Many terrorists today, she points out, are more “inclined to use highly lethal methods in order to destroy an impure world and bring about the apocalypse – unlimited ends lead to unlimited means” [2]. Thus the “new” terrorists seek to cause high numbers of casualties and are willing to commit suicide or use weapons of mass destruction in order to do so [2]. One only needs to consider the beliefs and concomitant actions of Timothy McVeigh in the 1995 Oklahoma City bombing of a federal building or Rev. Mike Bray and the abortion clinic bombings of the 1980s in the U.S.

This chapter examines the group psychology of terrorism. It begins with the premise that terrorism today is a group activity where members share a common ideology, group solidarity, and persecutory group identity.

Typically, the group ideology is fundamentalist and homogeneous, a totalistic system of beliefs that governs a way of life, which promotes group cohesion. Members merge via group solidarity behind the god-like image and grandiosity of their charismatic leader.

The terrorist group identity stems from a shared subjective experience of persecution among members of a common ethnic, religious, nationalistic or cultural group. This shared experience and collective memory (what Volkan [1] calls *chosen* trauma) fosters shame, anger, and a lethal perception of outsiders. These toxic sentiments are then fueled and solidified at historical moments of inter-group tension and vulnerability.

The essence of this bond of persecution symbolizes a shared experience of unjust treatment by *others*, specifically those outside of their ethnic, religious,

nationalistic or racial group. This fear of and hostility toward outsiders may simply derive from the others' rejection of the group's ideas and belief system, or it may emerge from the possible threat alleged of outsiders infiltrating and destroying the large-group identity (as is often the case in ethnic tensions). Inevitably, low group self-image and resentment for persecution and/or opposition (whether real or imagined) fosters a social structure of "us against them." The polarization of group insiders and outsiders is driven by the psycho-logic of large-group identity and requires further elaboration.

THE INTERNAL PSYCHO-LOGIC OF TERRORIST ACTS

Juergensmeyer [3] observes: "acts of terrorism are usually products of an internal logic and not of random crazy thinking. These acts of terrorism are done not to achieve a strategic goal but to make a symbolic statement." For Juergensmeyer what matters to terrorists is the symbolism, the theatrical nature of an act that draws world attention rather than a well-planned maneuver intended to defeat the *evil* enemy.

Ethnic, religious, cultural and nationalistic, large-group affiliations seem to provoke primitive thinking and extreme emotions, particularly when these groups contain fundamentalist ideologies and feel threatened and in danger of losing their common identity. In the minds of extremists, holding onto that identity and protecting the integrity and preservation of the group are worthy of self-sacrifice and thereby in the group mind, a threat, real or imagined, justifies violence and mayhem.

In Lifton's [4] study of Aum Shinrikyo, the Japanese cult that released sarin nerve gas in the Tokyo subways, he writes: "Any imagined Armageddon is violent, but the violence tends to be distant and mythic, to be brought about by evil forces that leave God with no other choice, but a total cleansing of this world. With Aum's Armageddon the violence was close at hand and palpable." Lifton continues: "Aum was always an actor in its own Armageddon drama, whether as a target of world-destroying enemies or as a fighting force in a great battle soon to begin or already under way. As time went on, however, Aum increasingly saw itself as the initiator, the trigger of the final event."

Similar to rightist American militia groups, these groups perceive themselves as destined to "save the world" and as Lifton points out, they are driven to do so even if the means necessary to meet their ultimate goal necessitates "destroying the world to save it." And, as is often the case, the vulnerable cult (or large-group identity) comes to believe in the evil of the *other* through processes of demonizing and dehumanizing the other and thereby rationalizing the destruction of the other as an act of God's will rather than mass killing. Psychologically, group members perpetrate murderous acts on outsiders when they come to view the *other* as non-human objects of evil (such as vermin, pests, and insects).

Staub [5] among others has noted that underlying the hostility and violence is a collective self-image of vulnerability. His research indicates in addition to group vulnerability that the presence of “difficult life conditions” and “certain cultural and personal characteristics” contribute to violent group activities such as genocide, terrorism, and ethnic cleansing. Difficult life conditions may include economic and political problems, crime, widespread violence, rapid changes in technology, social institutions, values, ways of life, and social disorganization. These conditions tend to promote feelings of powerlessness and confusion. In addition, cultural and personal characteristics provide further context for group violence and encompass low self-concept among group members. The group’s low self-concept and shared feelings of vulnerability then foster ingroup-outgroup differentiation (“us and them” mentality), exaggerated obedience to authority (as in authoritarianism), monolithic (vs. pluralistic) culture, emerging totalitarian or fascist ideology, and cultural aggressiveness. Staub also suggests that societal and political organizations with authoritarian and totalitarian characteristics are factors contributing to group violence.

Violent group members come to view themselves as potentially innocent victims of the other group’s (societal and political institutions) inherently evil nature – the psycho-logic of what psychoanalysts call “projective identification.” Projective identification is a mode of projection in which the subject locates part of him- or herself in someone else which permits knowing this person to have the projected attributes. At the same time, the other takes in the projected content to become like the projection. Controlling others (into which parts of the self are projected) is central to projective identification. Thus, group members are driven to act out in some fashion as a reaction to their imagined demise. In the case of projective identification, group members externalize and project all bad and evil attributes onto the image of the outsider’s group and its leadership. Eventually, the outsiders are depersonalized and dehumanized in the minds of the insiders. In some instances, the outsiders react with aggression and violence, which reinforces one groups’ image of the other and ties the volatile emotional knot between them – the essence of projective identification. And, as is the case with ethnic tensions, a vicious cycle of conflict is then set in motion with seemingly little hope of finding a peaceful exit. These are the dynamics of large-group identity.

DYNAMICS OF LARGE-GROUP IDENTITY

While we may prefer to avoid calling these violent acts (such as projective identification) “mad” or psychotic, we can benefit from exploring the underlying, primitive, motivating psychological dynamics of large-group identity. These large-group characteristics do in fact resemble psychotic processes. For example, group members’ devotion to totalistic ideologies and grand conspiracies are typical of (what psychoanalysts call) paranoid-schizoid processes of splitting objects into good and bad camps – viewing the world as black or white. Totalistic, absolutist,

and fundamentalist belief systems require compartmentalization and the psychology of splitting.

Group vulnerability and the impulse to act out is then triggered by anxieties further provoked by difficult life conditions that often reflect poverty and disenfranchisement; societal-cultural characteristics that foster and reinforce extremist and conspiratorial belief systems; and relatively recent political changes within the larger economic and social systems.

Beck [6] argues for distinguishing between the paranoid perspective of militia groups in the U.S. and mental illness: "The militants confine their conspiratorial beliefs to a relatively circumscribed domain: their relation with the government and their group. They have normal relations with members of their families and friends, carry on normal business transactions, and appear rational when testifying in court."

Nevertheless, Beck submits "although there are decided differences between people who are members of an extremist group and those who are psychologically disturbed, it is illuminating to examine the similarities in their beliefs and thinking. The comparison between militant group think and paranoid delusions is useful for the light it shines on the nature of the human mind and its tendency to create fantastic explanations for distressing circumstances" – what Freud observed as the human proclivity toward "magical thinking" – a tendency more commonplace in human groups. My approach to group violence and the development of a deeper understanding of the group mind or "group-in-the-mind" of terrorists shares Beck's assumption of a parallel with cognitive, psychotic processes.

Following this line of psycho-logic, Lifton [7] describes the phenomena of "doubling" and "numbing" in his extensive study of the Nazi doctors and their culpability for mass killings and genocide. Lifton reports that despite their horrific and murderous daily chores and the concomitant decision-making responsibilities, sentencing millions to death in gas chambers and many other millions to die in labor camps, he found that these same Nazi physicians were capable of carrying on relatively normal relations with their families – seemingly evil by day and apparently loving by night – a mental feat, he assumed was made possible by a combination of "doubling" and "numbing."

"Doubling" encompasses processes of (what psychologists call) psychological "splitting." Splitting describes a process in which the self-in-mind cognitively and emotionally splits apart good and bad images of the other based upon one's memories and experiences of the other. It is a form of internal compartmentalization and fragmentation of self and other. When internalized splits cannot be contained, the individual self projects, typically, bad images onto the other. This is what is meant by the psychological concept of projection. Fear, pain, and anguish often provoke these projections, leaving the self with the internalized good images. In large groups with common ideologies and emotional cohesion, these projections are commonplace under stressful and vulnerable circumstances. Numbing indicates a psychological distancing and desensitization of one's actions, despite their horrific nature. Hence, it is common for a perpetrator of a terrorist group to convey

that he felt nothing or has no remorse for his actions. His or her commitment to the grand idea, the ideology, provides a cognitive focal point that takes the self beyond the present experience of destruction and violence.

Under certain circumstances, joining a group may require relinquishing one's true self for the group's required ideological cloak, resulting in the performance of a false self among large group members something akin to Lifton's "doubling." For example, in *The Roots of Evil*, Staub [5] writes: "The greater the demands a group makes on its members and the more it guides their lives, the more completely the members can relinquish their burdensome identity and assume a group identity. However, submerging oneself in a group makes it difficult to maintain independent judgment of the group's conduct and more problematic to exert a contrary influence. De-individuation, a disinhibition of the usual moral constraint on individual action, is a likely consequence. Experiments show that aggressiveness is increased by conditions that weaken a sense of identity or increase anonymity, such as wearing masks." Stripping individuals of their distinct individuality and self-identity is correlated with increased aggression and violence. Group membership is acquired at a rather high cost of individual integrity and identity to self and much greater price to society in the members' ability to commit acts of murder and destruction without guilt or remorse.

The notion of "de-individuation" here has significance in human development. Cognitive and emotional growth and maturity occurs along a developmental path from infantile attachment (de-individuation) to childhood (early individuation) toward (eventual separation) relative adult autonomy. Hence, de-individuation signifies a psychologically regressive and backward process taking hold of the individual in his or her experience of group membership. Members of a group, when they regress in the face of stressful conditions, come close to experiencing their enemy as the original container of un-integrated bad parts (punishers) of their childhood selves. And as Volkan [1] points out: Such reservoirs typically contain nonhuman objects, such as a pig for a Muslim child or the turban for a Christian child. Similarly, adults, when regressed, reactivate a sense of experiencing the enemy as nonhuman.

Surrendering individuality and the capacity for critical judgment may promote group solidarity and identity while, at the same time, fostering a deeper underlying sense of powerlessness. While the group identity offers the illusion of compensatory power for its members, it is an illusion that does not solve the problem of members' deeper feelings of helplessness. Ultimately, this form of suppression is unsuccessful because powerlessness persists in the group's unconsciousness. Inevitably, group violence is a likely outcome.

Weston's [8] far-reaching study of Yugoslavia, as it was breaking up, provides a disturbing illustration of psychological splitting and regression within large (Serbian and Croatian) groups and their leaders' abilities to manipulate and provoke conflict between ethnic groups: "In Yugoslavia we found a strong tendency toward splitting. Images were split into good/bad and into we/them categories. Almost everyone idealized their own ethnic group and demonized others. The

black and white thinking was further encouraged by nationalistic leaders who actively played on group antipathy, using propaganda aimed at creating fear, rage and insecurity about people's safety." Slobodan Milosevic was successful at stirring up the hostilities of Serbs in Kosovo and promoting ethnic cleansing in just this manner. By evoking the collective memory of the 1539 Battle of Kosovo and insisting to his fellow Serbs that they will never be forced to leave Kosovo, Milosevic solidified the large-group against its neighboring enemy, the Ethnic Albanians in Kosovo.

TERRORISM AS A GROUP ACTIVITY: LARGE GROUP IDENTITY

Ethnic, religious, cultural and nationalistic groups are characterized by homogeneous subcultures in which psychological and physical boundaries between and among individual members seem to disintegrate and vanish from consciousness. The terrorist group identity and its concomitant belief system transcend individual identity of members themselves. The group and its leadership come to replace the ideals, fantasies, and ambitions of individual members. Thus, psychological processes of de-individuation abdicate power to the group and its leadership through emotional bonds that require intense loyalties and social cohesion.

In his article "The Origins of Ethnic Strife" Firestone [9] writes: "Identification with a particular ethnic or religious group is at once a powerful defense against death anxiety and a system of thought and belief that can set the stage for hatred and bloodshed. Conformity to the belief system of the group, that is, to its collective symbols of immortality, protects one against the horror of feeling the objective loss of self. In merging his or her identity with that of a group, each person feels that although he or she may not survive as an individual entity, he or she will live on as part of something larger which will continue to exist after he or she is gone." Joining the group and identifying with its leadership and ideology is a defense against death anxiety – the ultimate experience of individual vulnerability that leads to a merger (de-individuation) with the leadership and its associated large group identity. Firestone's application of the "defense against death anxiety" is synonymous with others' notion of group vulnerability and the perceived threat of outsider groups.

For example, Volkan warns: "When anxiety about identity occurs, members of a large group may consider killing a threatening neighbor rather than endure the anxiety caused by losing their psychological borders. In such a climate, chosen traumas and chosen glories, mourning difficulties, and feelings of entitlement to revenge are reactivated." These psychological processes underlie ethnic, racial, and religious acts of terrorism. A group's core identity is derived from the "pride" of attachment between members/followers and their leader(s). Members merge with like-minded blood-brothers, all of whom come to idealize their charismatic leader and his governing ideology. Yet, as is the case with individual pride, group pride is often a mask for group self-hatred and low self-concept.

LARGE GROUPS AND TOTALISTIC BELIEF SYSTEMS

These psychological processes of merger, de-individuation, and attachment then contribute to the leader's ideological influence over the actions of members. Individual morality and conscience are replaced by group ideology and worldview. Members forfeit their individual liberties for affiliation and identification with an omnipotent, god-like leader or guru who gives them hope of a better world.

Typically, group members come to adopt a totalistic and conspiratorial belief system that embodies the struggles of a cosmic war of good against evil. Once merger of individual and group leadership is complete, the psychology of splitting and paranoia – “us against them” – takes over. A persecutory group identity shapes and cements the members together through a common subjective experience and shared perception of evil and threatening outsiders. Primitive thinking and fantastic belief systems then promote group members unwitting resignation to simplistic solutions to otherwise complex societal problems. Enemies and scapegoats are identified, solidifying the group and targeting the aim of its aggression.

As Staub [5] notes: “History shows that people will sacrifice themselves to promote ideologies. Followers of ideologies identify some people as a hindrance and commit horrifying acts in the name of creating a better world and fulfilling higher ideals. This scapegoating occurs partly because the new social or spiritual order is defined in contrast to an existing order and partly because the ideal way of life is difficult to bring about or the new social system does not fulfill its promise.” Disappointment stirs resentment and anger. “Examples include the great blood bath after the French Revolution, the Inquisition and other religious persecutions, as well as genocides and mass killings.”

Whether it refers to religious affiliation, nationality, or ethnicity, large-group identity is defined as the subjective experience of hundreds of thousands or even millions of people who are linked by a persistent sense of sameness while also sharing numerous characteristics with others in foreign groups [1]. Our understanding of the concept of large-group identity begins with the work of Freud and, in particular, his view of group psychology and institutions.

In Freud's [10] *Group Psychology and the Analysis of the Ego*, he suggests that individual psychology and group psychology are not mutually exclusive. In particular he argues in this and in later works that our understanding of the intrapersonal world is derived from our knowledge of the psycho-dynamics of self and other from infancy through adolescence and adulthood – the internalization of interpersonal (self and other) experience over time. Thus, we come to learn that the emergence of one's sense of self and thereby one's sense of his or her core identity evolves from the mental internalization of self and other relations in dyads, groups, and institutions. In other words, our internalized subjective experiences, particularly those early on in life and through adolescence, then help to shape our mental images of oneself, others, and the world.

Leadership and authority are key components in our developing identity as they are central to our understanding of the nature of individual attachments and affiliations with large groups (religious, ethnic, and other primary associations) and nation-states. And, as Naimark [11] points out in *Fires of Hatred: Ethnic Cleansing in the Twentieth Century*: "Although the modern state and integral nationalism have been critical to ethnic cleansing in this century, political elites nevertheless bear the major responsibility for its manifestations. In competing for political power, they have exploited the appeal of nationalism to large groups of resentful citizens in the dominant ethnic population. Using the power of the state, the media, and their political parties, national leaders have manipulated distrust of the "other" and purposely revived and distorted ethnic tensions, sometimes long-buried, sometimes closer to the surface" (p. 10).

Naimark stresses the assumption of personal responsibility ultimately coming to rest on the shoulders of political elites, leaders. Yet leadership does not exist without followership. It is a dyadic relationship, merger of like-mindedness and shared responsibility. Naimark, however, is correct in pointing out the manipulative and influential power of leaders in large groups, which is critical and ought to be viewed as an appropriate starting point if we are moved to understand more deeply the phenomenon of group violence and hold accountable those most responsible. Consider the earlier example of Milosevic and his provocation of the Serbs against ethnic Albanians.

In Freud's original essay, he explains the dynamics of group psychology via the individual's attachment to the group. He argues that the individual surrenders his or her autonomy and independence to the group leadership by unconsciously replacing his or her own ego ideal with that of the leadership. In other words, group affiliation that may be characterized as hypnotic and suggestive takes place by a process in which the individual relinquishes to the leadership his or her own conscience, values, liberties and integrity. In joining the group, the self is forced into a psychologically regressive flight from individuality and autonomy to a more infantile state of de-individuation, merger, and social cohesion, which explains why we observe primitive thinking such as splitting and compartmentalization as well as shared fantasies and delusions among vulnerable large groups.

The group image of collective utopia is then represented for the membership by their loyalty and admiration of the group leader. So while Naimark [11] is correct in highlighting the responsibilities of political elites in fostering ethnic cleansing and other forms of violence, his analysis diminishes the role of followers in endorsing and empowering their leaders. As I stated it is a dyadic phenomenon and thereby ought to be examined and understood as such.

CONCLUSION

When large-groups, whether ethnic, religious, nationalistic or cultural, feel vulnerable, that is, when they feel the potential loss of their attachment and emo-

tional investment in the group's belief system and leadership, they fear the annihilation of the group-self or (what we have called) the large-group identity. Psychological regression is a common defense mechanism used by groups under these circumstances, whether the fear is legitimate or not, real or fantasized. Psychological regression and the associated cognitive and emotional splitting are typical responses to the experience of such profound anxiety (what Firestone calls death anxiety).

Under these conditions of psychological regression, members assume a collective, psychological flight behind their leaders into more primitive and infantile feelings. Charismatic leaders and gurus reflecting and articulating expansive visions and absolute ideologies, offer the illusion of a safe haven for the seemingly fearful, disenfranchised, and powerless members of society.

Group solidarity emerges from a foundation of ethnic, religious, cultural and nationalistic similarity and like-mindedness. There is safety in the comfort of the large-group identity and its god-like leader. The combination of homogeneity and group cohesion fosters de-individuation and de-differentiation in which members lose their individuality and sense of separateness. The loss of independence and critical thinking then reinforces polarized, compartmentalized thinking, which produces psychological splitting and regression among group members. It is this black and white, absolutist thinking rooted in infantile anxieties that fosters dehumanization of and violence against the *other*.

In the presence of social disorganization, economic and political problems, charismatic leaders can manipulate and provoke group violence by exploiting the "us and them" mentality of the large (ethnic, religious, cultural or nationalistic) group. By the identifying the enemy and then leading the group in attack against a popular scapegoat, terrorist leaders diminish followers' anxieties while proffering them a target for their long-held resentment and hostility.

REFERENCES

1. V Volkan. *Blood Lines: From Ethnic Pride to Ethnic Terrorism*. New York: Farrar, Straus and Giroux, 1997.
2. M Crenshaw. *The Psychology of Terrorism: An Agenda for the 21st Century*. *Political Psychology* 21 (2): 405-420, 2000.
3. M Juergensmeyer. *Terror in the Mind of God: The Global Rise of Religious Violence*. Berkeley: University of California Press, 2000.
4. RJ Lifton. *Destroying the World to Save It: Aum Shinrikyo, Apocalyptic Violence and the New Global Terrorism*. New York: Metropolitan Books, 1999.
5. E Staub. *The Roots of Evil: The Origins of Genocide and Other Group Violence*. New York: Cambridge University Press, 1992.

6. AT Beck. *Prisoners of Hate: The Cognitive Basis of Anger, Hostility, and Violence*. New York: Harper Collins Publishers, 1999.
7. RJ Lifton. *The Nazi Doctors: Medical Killing and the Psychology of Genocide*. New York: Basic Books, 1986.
8. WM Cullberg. When Words Lose Their Meaning: From Societal Crisis to Ethnic Cleansing. *Mind & Human Interaction* 8 (1): 20-32, 1997.
9. RW Firestone. The Origins of Ethnic Strife. *Mind & Human Interaction* 7 (4): 167-191, 1996.
10. S Freud. *Group Psychology and the Analysis of the Ego*. New York: Norton & Company, 1921.
11. NM Naimark. *Fires of Hatred: Ethnic Cleansing in Twentieth Century Europe*. Cambridge: Harvard University Press, 2001.
12. V Volkan. *Psychoanalysis and Diplomacy: Part 1. Individual and Large Group Identity*. *Journal of Applied Psychoanalysis* 1 (1): 29-55, 1999.

4

Aerosols: Fundamentals

Sudarshan K. Loyalka and Robert V. Tompson, Jr.

University of Missouri, Columbia, Missouri

INTRODUCTION

One cubic centimeter of atmospheric air contains approximately 2.5×10^{19} molecules. About 1000 of these molecules may be charged (ions). The molecules of N_2 , O_2 , and the various trace gases have sizes (diameters) of about 3×10^{-8} cm. The average distance between the molecules is about ten times the molecular size. In addition to the molecules and the ions, one cubic centimeter of air also contains a substantial number of particles varying in size from a few times the molecular size to several microns (μm , $1 \mu\text{m} = 10^{-4}$ cm). In relatively clean air there are about 1000 particles with diameters $0.001 \mu\text{m}$ to $50.0 \mu\text{m}$ while in polluted air there can be 100,000 or more, including pollen, bacteria, dust, and industrial emissions. These particles, which can be both beneficial and detrimental, arise from a number of natural sources as well as from the activities of the Earth's inhabitants. The particles can have complex chemical compositions and morphologies, and may even be radioactive or toxic. A suspension of particles in a gas is known as an aerosol. Atmospheric aerosol is of global interest and has an important impact on our lives.

Aerosols are characterized by a few fundamental properties. Most importantly, aerosol particles have large residence times (settling speeds on the order of a fraction of a cm/sec) and, because of their small size and large number, present a large surface area for interactions with the host medium. In addition, they can have a substantial effect on the transmission of light as they tend to occur in a size range that leads to substantial interaction (scattering and absorption) with light (see Fig. 4.1).

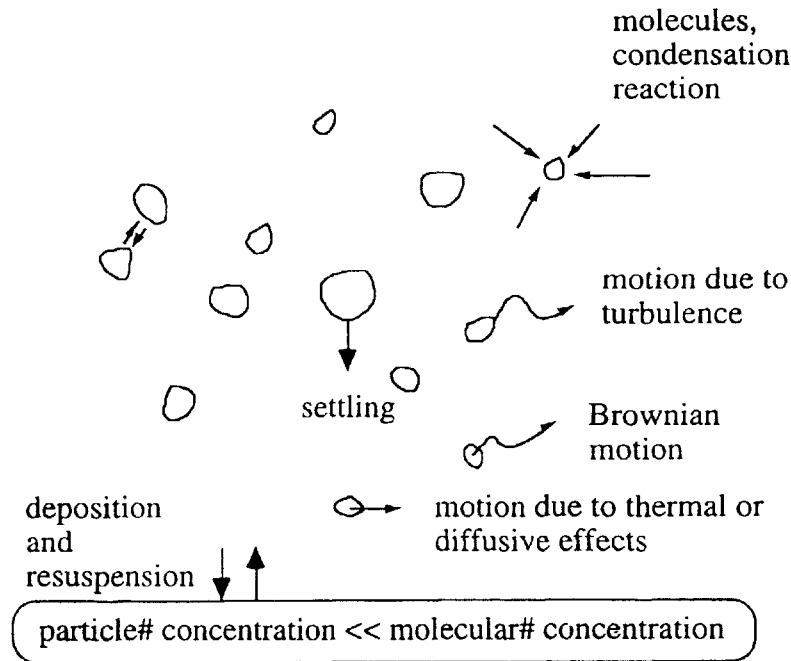


Figure 4.1 Aerosol interactions and motion.

For particles of a given composition, size and shape determine residence time as well as other dynamical properties that bear on particle removal by filtration or collection devices. Liquid particles are almost always spherical, but solid particles can occur in many different shapes varying from spherical to fibrous (needle-like forms). They can be chain-like agglomerates, or can be amorphous clumps. Typical size ranges of particles are shown in Fig. 4.2.

Usually, aerosol particles contain numerous species with varying physico-chemical properties. The compositions of the particles are determined by the processes that lead to their initial creation and their subsequent interactions with the host medium and electromagnetic radiation. Coarse particles ($\geq 2 \mu\text{m}$) are generally created by mechanical processes such as fragmentation and hence are rich in Ca, Fe, SiO_2 , and other constituents of the earth. Fine particles ($< 2 \mu\text{m}$) are generally derived from processes such as combustion or gas to particle conversion and are rich in C, Pb, sulfates, and ammonium and nitrate ions. The trace and often toxic species such as As, Cd, Cs, Sr, Zn, and Se are also mostly concentrated in the fine particles. Nuclear explosions create large numbers of radioactive particles that can disperse globally. Volcanic eruptions lead to particles, some of which reside in the atmosphere for years.

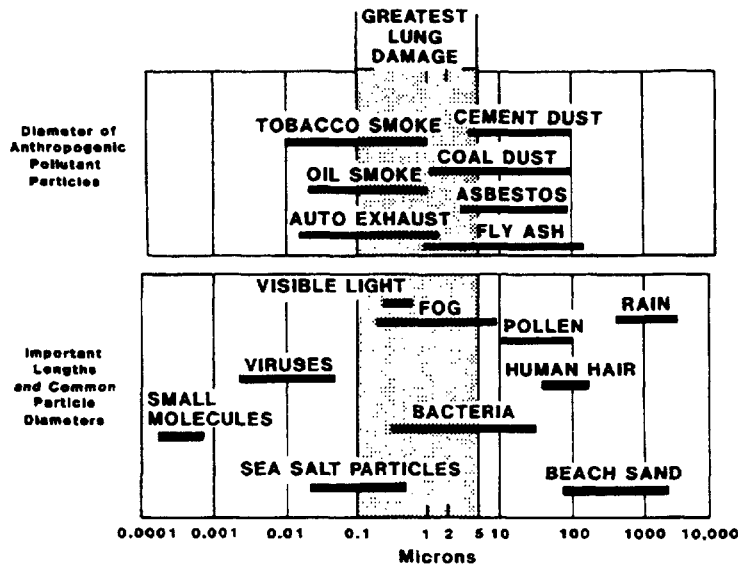


Figure 4.2 Typical size range of aerosols [1].

Since the number of particles in an aerosol is large, and since each particle can have a multitude of physical and chemical characteristics, a description that accounts for particles individually is not sought. Rather, one focuses on the important attributes of the aerosol and considers a distribution function based on particle properties and size. It has been observed in many applications that the aerosol distributions are close to some simple forms.

The distribution of chemicals with respect to particle sizes is, indeed, quite complex. One also observes complex surface distributions of different species on particle surfaces. Chemicals are transported to different locations in human respiratory tracts as dictated by different particle sizes, and these speciations play a major role in the delivery of toxic dosages to specific cells in human lungs. The atmospheric environment can be viewed as a giant and complex chemical reactor. Control strategies require sound scientific understandings at both microscopic and macro-scales in time and space, and interplay of theory, modeling and experiments.

To consider a simple example, a person breathes about 20 m^3 of air per day. Even if there were 1 particle/cm^3 of air, a person would breathe about 20 million particles in a day, or about a million in an hour. Particle concentration in a polluted city may be about $100 \mu\text{g/m}^3$. Suppose these particles have a diameter of $0.1 \mu\text{m}$, and density of 1 gm/cm^3 . Then there would be about $2 \times 10^5 \text{ particles/cm}^3$ of

air. Hence a person would be breathing about 4000 billion particles per day. Of course the particles are distributed over a size range, and a large number deposits in the upper respiratory tract. Still a sufficiently large number reaches the lower respiratory tract, and also interacts with the large surface there (see Fig. 4.3). Thus aerosols, with chemical, radioactive, or biological implications for lungs, are particularly attractive to terrorists. The aerosols also deposit externally on the human body, and cause reactions there also.

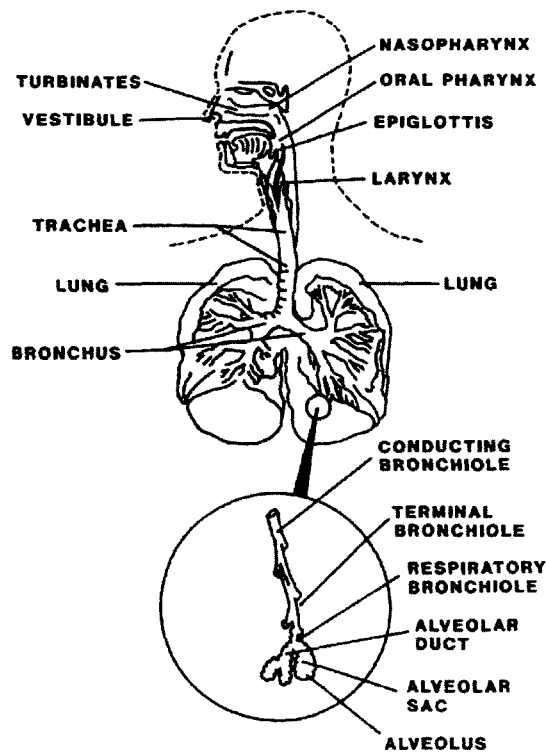


Figure 4.3 The human respiratory tract.

We will describe in this chapter some fundamental properties of aerosols, and then discuss how they are generated and dispersed in the atmosphere and in confined spaces. We will also discuss how particles are sampled and characterized. These understandings lead to means by which one can guard against terrorist actions that seek to disperse aerosols.

The most important aspect of aerosol particles is, perhaps, their interaction with gas molecules. Under standard conditions, a current of 10^{23} gas molecules/cm²sec impinges on a particle and, in equilibrium, a current of the same magnitude is returned back from the particle's surface to the surrounding gas. Generally, the molecules incident on a particle's surface can react with the particle constituents, they can be absorbed or adsorbed, or they can be scattered back into the gas (see Fig. 4.4). For an isolated single particle in an infinite expanse of a stationary gas and in absence of gravity and other forces, one would assume that the particle would not move.

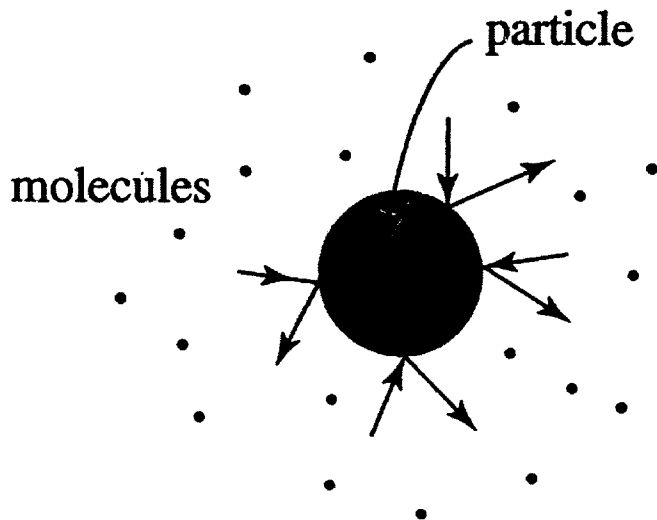


Figure 4.4 Molecular interactions with a particle.

But this is not true, as the molecules incident on the surface of a particle impart impulse to the particle, and while on the average there is no net force on the particle, there is a fluctuating force. The particle moves randomly ("diffuses") under this force, with a velocity determined by this force and an opposing force due to friction exerted by the gas (or the molecules through which the particle moves). This motion is known as the Brownian motion, and its quantitative aspects were first clarified by Einstein and Smoluchowski. Using the nomenclature,

T	temperature of the environment (K)
B	particle mobility ($T M^{-1}$)
D	diffusion coefficient ($L^2 T^{-1}$)
d_p	particle diameter (L)

g	acceleration due to gravity ($L T^{-2}$)
L	characteristic dimension of a body or flow (L)
m	particle mass (M)
U	characteristic flow speed ($L T^{-1}$)
V_s	sedimentation velocity ($L T^{-1}$)
x	some arbitrary distance (L)
λ_c	molecular mean free path (L)
μ	fluid dynamic viscosity ($M L^{-1} T^{-1}$)
ρ	fluid mass density ($M L^{-3}$)
$\tau = m B$	relaxation time (T)
Kn	Knudsen Number, $Kn = \lambda_c / d_p$
C_c	Cunningham Correction Factor, depends on Kn
n	Particle concentration (L^{-3})
J	Particle current ($L^{-2} T^{-1}$)
S	Particle source ($L^{-3} T^{-1}$)
<u>Units</u>	K–temperature, L–length, M–mass, T–time

The frictional force F_D is given as:

$$F_D = 3\pi\mu d_p v / C_c$$

where v is the instantaneous velocity of the particle. The diffusive motion of the particle (see Fig. 4.5) is determined through a “diffusion” coefficient,

$$D = BkT$$

where k is the Boltzmann constant, and B is the “mobility” (defined as velocity/force) of the particle, and is given as:

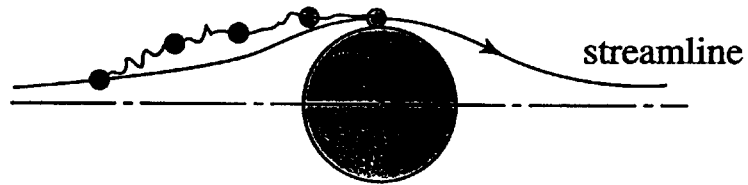
$$B = v / F_D = \frac{C_c}{3\pi\mu d_p}$$

The root mean square distance traveled in time t by a particle undergoing linear (one-dimensional) diffusion is expressed as:

$$x = \sqrt{2Dt}$$

Particles also move under external forces, and in particular all particles settle under gravity (see Fig. 4.6). The particle motion under an external force can be described by the equation:

Small particles: Brownian motion (diffusion)



Large particles: Inertia

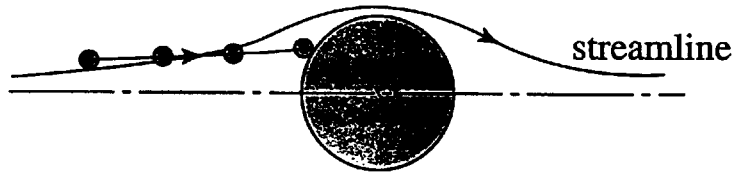


Figure 4.5 Aerosol diffusive and inertial motion.

$$m \frac{dv}{dt} = F - \frac{v}{B}$$

Or,

$$\frac{dv}{dt} = -\frac{v}{\tau} + \frac{F}{m}; \quad \tau = B m$$

Where τ is known as the relaxation time, and it is a measure of how quickly the particle adapts to a flow. The settling velocity V_s is thus simply given as:

$$V_s = B m g = \frac{m g C_e}{3\pi\mu d_p}$$

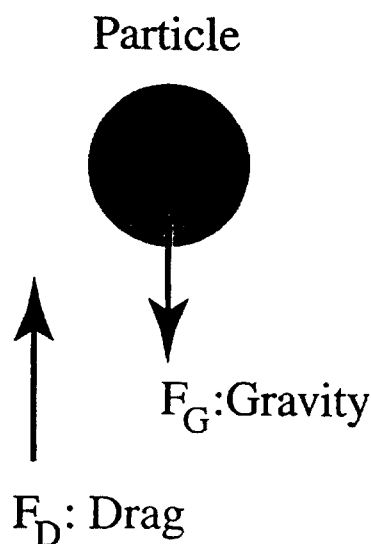


Figure 4.6 Aerosol motion: gravity and drag.

Table 4.1 shows typical values of the quantities discussed here. We note that the smaller the particles, the more rapidly they diffuse and the more slowly they settle. Thus particles of intermediate size are likely to remain suspended for the longest time, as the larger particles settle out, and the smaller particles attach to other larger particles or deposit on surfaces. We should emphasize that particles do move with air (gas) flow - the convective motion (or the mean speed of flow), and the diffusive and gravitational motions are superimposed on this convective motion. In fact this convective motion (e.g., plumes) is the principal means of aerosol dispersion in most cases. Also, the convective motion (e.g., breathing, spraying) is the principal means of deposition, as it brings particles near surfaces whence particles deposit because of diffusion and settling, and other forces.

As we have noted, particles grow because of condensation of water vapor; they can also diminish in size because of evaporation. They can react with gases and vapors, and they can coagulate (adhere) when they collide with other particles. The particles can fragment, and also react with sunlight and other radiation. Bioaerosols may not survive because of atmospheric conditions, or internal causes. Radioactive particles can decay, and charged particles can have a host of other reactions. Particles adhere to or repel from surfaces because of short range molecular forces. They can be charged, and they can also accumulate ions. They can mediate transport of many molecular species. All the processes are complex, and

in addition to deposition, these affect aerosol evolution and dispersion, and the aerosol uptake by humans and animals.

Table 4.1 Aerosol properties as a function of size of a unit density sphere in air at Standard Temperature and Pressure (STP).

Particle Diameter (μm)	Sedimentation Velocity (cm/sec)	Diffusion Coefficient (cm^2/sec)	Mobility (sec/g)	Particle Relaxation Time (sec)
d_p	$V_s = \frac{m g C_c}{3\pi \mu d_p}$	$D = B k_B T$	$B = \frac{V_s}{m g}$	$\tau = m B$
0.001	6.5530E-07	5.1084E-02	1.2719E+12	6.6595E-10
0.01	6.6901E-06	5.2312E-04	1.3025E+10	6.8197E-09
0.1	8.6316E-05	6.7494E-06	1.6804E+08	8.7988E-08
1.0	3.5054E-03	2.7410E-07	6.8245E+06	3.5733E-06
10.0	3.0605E-01	2.3931E-08	5.9583E+05	3.1198E-04
100.0	2.4844E+01	2.3583E-09	5.8717E+04	3.0744E-02

These fundamental properties play the most important role in particle filtration and removal. Fine particles are preferentially removed by fabric filters and electrostatic devices, while large particles are removed through use of cyclones and impactors. Intermediate size particles ($\sim 0.3 \mu\text{m}$) are harder to remove as they neither diffuse as well nor settle as much. Generally for all efficient filtration one needs high volume flows. Particles can also be scavenged by use of sprays and mists. We also know that heat and sunlight can dissipate fogs.

GENERATION

Fogs, mists, power plant plumes, automobile exhaust, cigarette smoke, fire and combustion, pollen, dust, bacteria and viruses are part of our common experiences. Fine aerosols generally form through nucleation and condensation/reaction processes in the environment as well as combustion. Coarse particles arise from many mechanical processes and human activities.

A fire will invariably lead to large aerosol production. We know that explosions lead to dense aerosol (large concentrations) release. Burning some oils is an effective way of producing large quantities of aerosols. Crop-dusters release large amounts of pesticides in aerosol form. Sprayers or blowers can also generate large amounts of aerosols. Volcanic eruptions and nuclear explosions release huge amounts of aerosols. Violent destruction of buildings releases copious amounts of aerosols through combustion as well as fragmentation.

Bioaerosols (viruses, bacteria, pollen, etc.) can be generated in laboratories, stored, and then injected into the environment through use of sprayers, dusters, blowers, balloons, or explosives.

DISPERSION

Aerosols disperse more rapidly with wind, but they disperse even in the absence of the wind. We recognize that in open environments, release at a greater height, as well as wind, lead to greater dispersion of aerosols. We can determine the direction of wind, as well as estimate its turbulence, by watching the movement of the plume (fine particles are used in wind tunnels etc. to visualize flow). We know that rain washes out aerosols from the atmosphere. We also know that air currents or human activities can cause resuspension of dust from surfaces, and then disperse it in the environment. Quite clearly in confined environments (homes, offices, factories, shopping malls, airports, automobiles, train stations) aerosol dispersion is strongly influenced by the ventilation (air exchange, flow and filtration) and heating/air-conditioning systems, and a release of aerosols into a ventilation system could be a very effective means of dispersing them. In open environments, wind patterns, height of release, humidity and rain, sunlight, etc. play important roles. We should note, though, that fine particles are generally likely to disperse very widely in the open if released at multiple points (to avoid coagulation inherent in a dense aerosol, which leads to larger particles and greater settling near the source), a good height, and in low humidity (to avoid growth and coagulation or reactions) and in the absence of rain (to avoid washout).

Sophisticated physico-chemical and mathematical descriptions of aerosol dispersion have been studied. Computer programs are being developed that would make possible semi-realistic and real time computations of aerosol dispersion. Neglecting aerosol coagulation and growth processes, an equation that can provide simple and suitable description of aerosol dispersion and deposition, can be written as:

$$\frac{\partial n}{\partial t} = -\nabla \cdot \mathbf{J} - \mathfrak{R}n + S$$

where S is the particle source, and the particle current can be written as,

$$\mathbf{J} = \mathbf{U}n - D\nabla n + \mathbf{V}_s n$$

Here n is the particle concentration, and it could be a function of position, and time, as well as particle size. \mathbf{U} is the convective velocity, and the flow could be turbulent or laminar, depending upon the conditions. The flowfield can be estimated or calculated from the flow conditions and appropriate fluid dynamic equations. We have included a removal rate constant \mathfrak{R} in the equation to indi-

cate additional removal (death for example of a bioaerosol or washout) of particles. This equation will be subject to appropriate initial and boundary conditions. Solutions of this and/or a spatially homogenized equation provides considerable insights into aerosol concentration over the space of interest. The major points of departure from the dispersion of a gaseous contaminant are the presence of settling and comparatively low values of diffusion coefficient. There exist many popular descriptions of gas dispersions, and for short times, these provide useful descriptions of aerosol dispersion also.

Let us consider for example, dispersion of aerosols resulting from a nuclear weapon explosion. The explosion leads to vaporization of the weapon material within fractions of a second. If it is a near surface explosion then the surface material (soil, water, structures) in the vicinity is also immediately vaporized and suspended. This material is cooled as the fireball expands. It condenses, and forms into fine particles which will contain radioactive species such as cesium, iodine, strontium, uranium, molybdenum, plutonium, etc. These fine particles disperse, and eventually settle out depending upon the heights at which these are formed, and the wind patterns involved. Particles formed high in the atmosphere could travel around the globe. Since the explosion will set off structures/wood on fire within a few miles, these fires would contribute additional smoke aerosols, upon which radioactive species would condense or attach. These smoke aerosols would also undergo further dispersion and settling/diffusion. Thus a nuclear explosion would result in some immediate and some long term "fallout" of particles, both near the explosion and far away from it. We know from weapons tests that wind directions and weather conditions can change the course of fallout immensely.

SAMPLING AND CHARACTERIZATION

The fundamental dynamic properties of aerosols dictate their sampling. For the same speed of flow, coarse (heavier) particles have greater inertia than those of fine (lighter) particles, and hence any change in flow direction can cause coarse particles to deposit on a collection surface preferentially (that is, fine particles have a low relaxation time, and they adjust to change in flow more rapidly, and do not depart from streamlines that easily). But particles of almost all sizes can be collected in samplers that employ high speeds. A continual variation in flow speeds can be employed for size-specific deposition of aerosols on collection plates. A device based on this principal is known as an aerosol impactor, and a schematic is shown in Figure 4.7. Generally one employs one or several (two, six, or more) stages, and collects particles on filters or growth media for bioaerosols (agar for example). The physical, chemical and biological properties of the collected particles can be obtained in laboratories from a number of analytical methods such as gravimetry, optical and electron microscopy, neutron activation analysis, spectroscopy, and DNA sequencing.

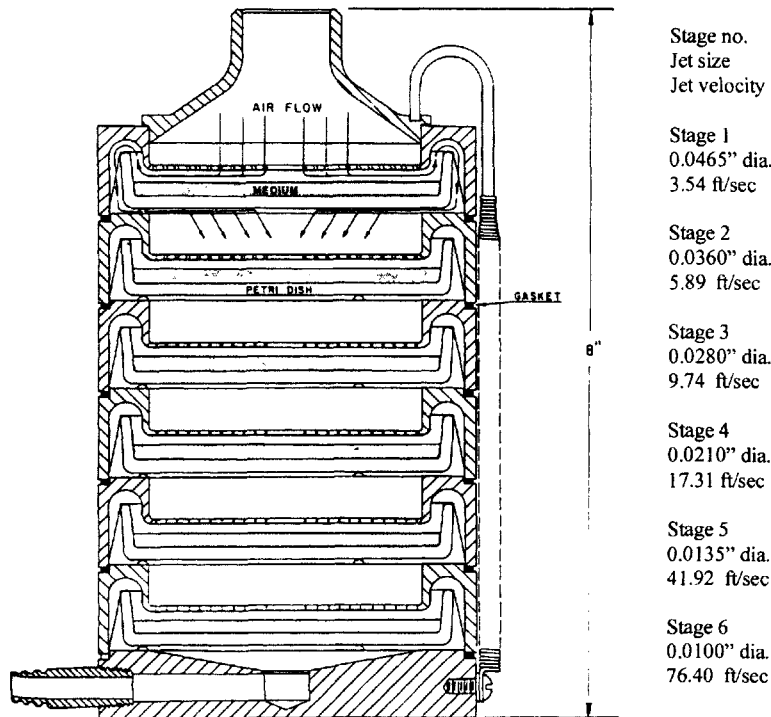


Figure 4.7 Schematic diagram of a six-stage Andersen sampler [2].

Quite often, for bioaerosol sampling, one also employs liquid impingers. Here the aerosol is flowed at sonic speed through a liquid medium, thus resulting in high collection rates. The liquid is the collection medium, and the particles collected in it can then be conveniently analyzed in laboratories.

For collection of fine, and ultra fine particles, with low particle concentration, impaction may not be very effective. Here one can employ fabric bags (narrow passages lead to high deposition because of diffusion) or electrostatic devices (that charge and then collect particles).

The sampling and characterization are always of limited value if the sample size is small, and if characterization is affected for example by the viability of a sample (for bioaerosols). Improved methods of non-destructive and rapid testing are areas of current research interest. An important challenge is identification of the source of aerosols, as the collected aerosol particles could be substantially different from the particles that are generated (the primary aerosol).

REFERENCES

1. AL Hines, TK Ghosh, SK Loyalka, RC Warder. *Indoor Air: Quality and Control*. New Jersey: Prentice Hall, 1993.
2. AA Andersen. New sampler for the collection, sizing, and enumeration of viable airborne particles. *J Bacteriology* 76: 471-484, 1958.

BIBLIOGRAPHY

- CN Davies. Editor. *Aerosol Science*. London: Academic Press, 1966.
- R Dennis. *Handbook on Aerosols*. Washington, D.C.: U.S. Department of Energy, 1976.
- SK Friedlander. *Smoke, Dust and Haze*. New York: Wiley, 1977.
- NA Fuchs. *The Mechanics of Aerosols*. New York: Pergamon, 1964.
- GM Hidy. *Aerosols, An Industrial and Environmental Science*. New York: Academic Press, 1984.
- GM Hidy, JR Brock. Editors. *Topics in Aerosol Research*. Vols. 1-3. Oxford: Pergamon, 1972.
- WC Hinds. *Aerosol Technology*. New York: Wiley, 1982.
- WH Marlow. Editor. *Aerosol Microphysics*. Vols. I-II, New York: Springer-Verlag, 1982.
- J Seinfeld. *Atmospheric Chemistry and Physics of Air Pollution*. New York: Wiley, 1986.
- S Twomey. *Atmospheric Aerosols*. New York: Elsevier, 1977.
- MMR Williams, SK Loyalka. *Aerosol Science: Theory and Practice, with Special Applications to the Nuclear Industry*. New York: Elsevier, New York, 1991. (A part of the introduction follows from this text).

5

Biological Agents: Effects, Toxicity, and Effectiveness

Gordon D. Christensen

*Harry S. Truman Memorial Veterans Hospital and
University of Missouri, Columbia, Missouri*

INTRODUCTION

Over the history of mankind, military organizations have occasionally used biological agents as weapons. With the advent of microbiology in the 20th century, multiple national research and development programs have applied microbes to the creation of weapons of mass destruction. In recent years, terrorist organizations – particularly organizations with strong religious affiliations – have also begun deploying biological weapons. Fortunately, the capacity to create sophisticated biological weapons and carry out a massive biological attack appears to be beyond the resources of most terrorist organizations. Unfortunately, these organizations seem unrestrained by the humanitarian concerns that normally limit biological warfare. In the last two decades we have witnessed an increase in the number and lethality of bioterrorist attacks, raising the spectre of a successful large-scale attack in the future. To prepare for the worst, we must anticipate the agent the bioterrorist will use in an attack. While ‘germ’ warfare and ‘bioterrorism’ have different goals and different limitations, they often use the same biological agents for weapons. Six organisms appear to be the weapons of choice: anthrax, smallpox, plague, tularemia, hemorrhagic fever, and the toxin from *Clostridium botulinum*. The following pages examine in greater detail the background and limitations of bioterrorism, the variety of weapons in the biological armory, and the specific bacteriologic and clinical features of these six potential terrorist weapons.

BACKGROUND

To defend ourselves from bioterrorism we must anticipate which biological weapon the bioterrorist will use and how the bioterrorist will employ the weapon.

Biological weapons use a microorganism or a toxin derived from a microorganism to produce death or disease in humans, animals, or plants. Over the years humans have employed a large number of biological agents to cause destruction, but the arsenal for bioterrorism is not the same as the arsenal for biological warfare. The difference lies in the difference between the goal of bioterrorism and the goal of biological warfare.

The goal of biological warfare is to eliminate or incapacitate the enemy. The goal of bioterrorism is to instill fear in the enemy in order to achieve a political goal or promote an ideology¹ [1]. Illness, death, and destruction may result from the bioterrorists' activities, but these casualties are only a secondary concern. For this reason the bioterrorist has a wider selection of biological weapons than does the combatant preparing for biological warfare [2].

Biological warfare uses either weapons of mass destruction or small-scale weapons. Weapons of mass destruction are targeted against an armed force, civilian population, or national economy². Small-scale weapons are targeted against an individual, a unit, or a facility. Either way, the military use of biological weapons has tactical, strategic, financial, and political considerations that determine the selection and deployment of the biologic agent. For tactical reasons the weapon must be of military grade, meaning the munitions have known performance characteristics such as lethality, range, and shelf life. This requires a large research and development program. For strategic reasons weapons of mass destruction must be safely produced in large quantities. This requires a major manufacturing plant capable of handling large volumes of biohazardous materials. Both large scale and small-scale weapons require safe storage in secure locations, this requires guarded armories designed to store biological weapons. Since civilization universally condemns biological weapons as immoral and cruel, the weapons program must be kept secret. Only a few nations have the financial resources and political structure to fund and hide the research and development program, manufacturing plant, and armories required for biological warfare.

To use military grade munitions, the bioterrorist must have either stolen the weapon or had it given to him. Because the existence and location of the weapons

¹ In addition to warfare and terrorism, biological weapons can be used to commit criminal acts or 'biocrimes.' Biocrimes include crimes against individuals for personal gain or revenge [1] as well as mischievous acts by disturbed individuals.

²The focus of this chapter is on anti-personnel weapons. Bioterrorism, however, also includes the use of biologic agents to destroy livestock, crops, and machinery.

are both secret and secure, these armaments are rarely stolen. Stolen weapons suggest an 'inside job' with only a small amount of material available to the thief³.

The terrorist may receive a military grade weapon as a gift because the provider shares goals with the bioterrorist. An outright gift of a weapon of mass destruction is probably rare, because the gift would jeopardize the provider's biological weapons program to public exposure and condemnation. While gifts of small-scale weapons pose less danger of public censure, such gifts would also have a diminished capacity to cause terror.

For these reasons bioterrorists will often use weapons fabricated by themselves with or without the assistance of national agencies. This can be accomplished at a low cost, but the product will most likely be unsophisticated [2, 4], available in limited quantities, with unknown and variable properties such as lethality, range, and shelf life. Also, like building a bomb in one's basement, the homebuilt biological weapon could 'blow-up' during assembly, meaning the bioterrorists themselves have a substantial risk of succumbing to their 'weaponized' infectious disease [4]. For suicidal terrorists this may not pose a problem or may even be the objective, but for all others the potential for accidental 'occupational' illness will place limitations on the choice, manufacture, and deployment of the weapon.

Strategic, tactical and financial constraints on bioterrorism can be simply avoided by using the ruse of a biological weapon to create terror. Because of the ease and inexpense of manufacture this is the weapon of choice for many bioterrorists. While such a weapon has no capacity to produce illness and death, it can cause tremendous fear and publicity because the victim does not know the weapon is a hoax. The bioterrorist seeks fear and publicity, but repeated use of such a fraudulent weapon can rapidly extinguish the fear and even lead to ridicule or scorn.

Focus on anthrax hoaxes. Many biological hoaxes have threatened the use of anthrax [1]. For example, in February 1998 Larry Wayne Harris boasted to an informant that he had enough military grade anthrax to "wipe out" Las Vegas [4, 5]. A member of the white supremacist group 'Aryan Nation,' Harris was a registered microbiologist and the author of a self-published Internet book "Bacteriological Warfare – Major Threat to North America" [5]. He had previously been convicted in 1995 for fraudulently obtaining three vials of freeze-dried *Yersinia pestis* for \$240 from the American Type Culture Collection [5]. For these reasons the Federal Bureau of Investigation (FBI) took the boast seriously. But the FBI found that Harris had only an avirulent vaccine strain of anthrax in his possession, a strain incapable of

³ For example, the Associated Press recently reported that in 1992 an internal audit of stocks found missing specimens of anthrax, Ebola virus, and other pathogens at the Army's biological warfare research center [3].

producing illness [4]. Nevertheless, this incident provoked considerable public angst and publicity; it also provoked a proliferation of ‘copycat’ anthrax hoaxes through the rest of 1998 and 1999 [4]. For example, on reviewing public domain reports of anthrax incidents, Jessica Stern found just two such incidents for the period 1992-1997. After the 1998 Harris incident, however, she counted 37 anthrax incidents in 1998 affecting some 5,500 people [4]. These hoaxes included anonymous letters purporting to contain anthrax sent to medical clinics in Indiana, Kentucky, and Tennessee and anonymous threats of using anthrax to contaminate the air-handling systems for various public buildings in California [6].

Likewise, after the attack on the World Trade Center and the subsequent mailing of military grade anthrax to political and media targets, the general public had a heightened awareness of bioterrorism. In this setting numerous ‘copycat terrorists’ found ample opportunity to cause additional terror and mischief simply by labeling innocent powders as ‘anthrax’ and then sending the material with threatening letters to their victims. Based on a telephone survey of health departments over the period September 11 to October, the Centers for Disease Control and Prevention (CDC) estimated that United States health departments had received an estimated 7,000 reports of potential bioterrorist threats [7]. In comparison, the number of anthrax threats reported to federal authorities during 1996-2000 did not exceed 180 [7].

As noted above, the community of nations regards biological weapons as inhumane, unnecessarily cruel, and fabulously dangerous. Nations that openly manufacture such weapons – such as Iraq – expose themselves to public censure and preemptive strikes by other nations to eliminate the terrifying program [8]. These political considerations might not restrain militaristic religious and extremists groups from considering bioterrorism [4]. Such terrorist organizations do not respect governmental authority because they view secular rulers and the law they uphold as illegitimate [4]. The terrorists’ objective is to destroy the legitimacy of the government by creating as much fear and chaos as possible [4]. The terrorists do not fear public censure for their misdeeds because the terrorists believe their actions please God and they consider their victims to be subhuman because the victims do not subscribe to the terrorists’ religious beliefs [4]. Stern noted that in the last decade the number of terrorist acts committed by religiously motivated groups has increased and the acts have become more violent [4]. From this perspective it is easy to understand why authorities view with such alarm the credible threats of bioterrorism made by emerging militaristic religious orders like the white supremacist groups, Aum Shinrikyo, and Al Qaeda.

So what weapons does the bioterrorist include in the biological arsenal? Our examination of this armory begins with the history of biological weapons and concludes with a review of prospective agents.

HISTORICAL USE OF BIOLOGICAL WEAPONS

Probably because of a poor understanding of biology, prior to World War I combatants infrequently used biologic agents with uncertain results [9]. Characteristically, these attempts used simple devices to spread contaminated material or expose individuals to hazardous materials. For example, ancient history records that the Carthaginian leader Hannibal hurled clay pots filled with venomous snakes onto the decks of an opposing naval force; the resulting chaos allowed Hannibal to rout the enemy [10]. Medieval history includes multiple attempts to use plague as a weapon; during the siege of Caffa the Tartars threw the carcasses of plague victims into the fortified town expecting to cause an outbreak of the plague [8, 10]. The history of the New World includes several attacks on the Native American population with smallpox [10]. During the French Indian War, the British distributed contaminated blankets to French loyalist Native Americans; the blankets had been previously inoculated with the crusts from smallpox lesions with the expectation of causing an epidemic of smallpox [8, 10]. Throughout human history combatants have used animal carcasses, cadavers, and sewage to practice a simple form of biological warfare. By dumping the putrid material into an enemy's drinking water supplies, the attackers expected to incapacitate their adversaries with fouled water [8-10]. During the Vietnam War, the Vietcong practiced another elemental form of biological warfare using a strategy also employed by many other peoples in many other situations. The Vietcong dug pits and lined the bottoms with bamboo and wood spikes soiled with human feces, expecting unwary passers-by would fall into the pits, impale themselves on the sticks and develop severe wound infections [8, 11].

The advent of microbiology provided specific agents for conducting biological warfare. During World War I the Germans reputedly tried to sabotage cavalry horses in Baltimore with glanders and military pack mules in Rumania with both glanders and anthrax [10]. During World War II, the Japanese conducted an extensive program for the development of biological weapons, reputedly resulting in the deaths of some 10,000 prisoners [8]. The Japanese reportedly used a variety of agents to attack China, including contaminated foodstuffs, drinking water, and air, as well as plague-infected fleas [8, 12]. Some of these attacks backfired; in an attack on Changteh in 1941 the Japanese forces reportedly suffered 10,000 casualties and 1700 deaths due to their own biological weapons [8]. More recently in 1984 members of the Bhagwan Shree Rajneesh commune attempted to incapacitate voters in a local election with food poisoning by contaminating salad bars in Dalles, Oregon with home grown *Salmonella typhimurium* [9].

Even though the Geneva Protocol of 1925 and the 1972 Biological Weapons Convention specifically banned biological warfare, after World War I a number of nations – including treaty signatories – used the new science of microbiology to establish large programs for the discovery, development, and production of biological weapons [10]. Propelling this development was the promise of developing indefensible weapons with the capacity to cause massive destruction, primarily

through the dissemination of infectious aerosols. As a result national research programs explored the military utility of numerous agents, but only a small number appear to have become serious candidates for conversion into weapons, *i.e.* 'weaponized' (Table 5.1) and even fewer have been actually deployed (Table 5.2) [9, 11].

Table 5.1 Prospective agents of biological warfare in the modern era, adapted from [2, 8, 9, 11, 13].

Disease	Agent	national arsenal	CDC risk category
Viral encephalitis	Particularly Venezuelan equine encephalitis	US & USSR	B
Agents of viral hemorrhagic fevers	Including Marburg and Ebola	USSR	A
Smallpox	<i>Variola major</i>	USSR	A
Typhus	<i>Rickettsia prowazekii</i>	USSR	unranked
Q fever	<i>Coxiella burnetti</i>	US & USSR	B
Brucellosis	<i>Brucella suis</i>	US	B
Tularemia	<i>Francisella tularensis</i>	US & USSR	A
Glanders	<i>Burkholderia mallei</i>	USSR	B
Melioidosis	<i>Pseudomonas pseudomallei</i>	USSR	B
Plague	<i>Yersinia pestis</i>	Japan & USSR	A
Cholera	<i>Vibrio cholerae</i>		B
Food poisoning	<i>Clostridium perfringens</i>		unranked
Enterotoxin B	From <i>Staphylococcus aureus</i>	US	B

Tables 5.1 and 5.2 also include abbreviation for the United States of America {US}. This entry indicates the US reportedly included this agent in our biological arsenal before President Nixon unilaterally banned the use of offensive biological weapons in 1969 and had all stocks destroyed by 1973 [8, 15].

Also included in Tables 5.1 and 5.2 is abbreviation for the former Soviet Union (Union of Soviet Socialist Republics) {USSR} indicating that the USSR reportedly included this agent in their arsenal of biological weapons [11, 13]. The Soviet Union selected agents and toxins for possible weaponization by scoring each candidate for infectivity, toxicity, environmental stability, ease of large-scale manufacture, disease severity, and stability in the atmosphere [11].

Table 5.2 Deployed agents of biological warfare in the modern era, adapted from [11, 13, 14].

Disease	Agent	CDC risk category	Deploying Nations	Conflict
Anthrax	<i>Bacillus anthracis</i>	A	multiple nations and conflicts	US & USSR
Assassination	Ricin toxin	A	USSR	Cold War
Botulism	<i>Clostridium botulinum</i> toxin	A	Iraq (Persian Gulf War)	US

Focus on Fort Detrick. In 1942 the US Army Chemical Warfare Service began an offensive and defensive biological weapons research program headquartered at a small National Guard airfield named Camp Detrick (later renamed Fort Detrick), Maryland [15]. The field became the location for extensive laboratories and testing facilities, including a 1-million-liter, 40-foot-high steel sphere known as the “Eight Ball.” Between 1954 to 1973 Fort Detrick enrolled some 2,300 volunteers – primarily Seventh-day Adventists – into a human research program known as “Operation Whitecoat” [16]. In some experiments, investigators detonated biological weapons in the Eight Ball and then exposed the volunteers to the aerosols [8, 16]; other experiments tested new vaccines and therapeutic agents [16]. The sphere remains today as a historical monument to the program [15]. Ultimately the Fort Detrick investigators determined that with great effort biological weapons could be safely produced and effectively deployed [15], in the process they developed modern principles of biosafety and containment [15]. Between 1943 to 1969, Fort Detrick workers acquired 456 cases of illnesses from their work; three patients died, two with anthrax and one with encephalitis [8]. Currently the Fort Detrick facilities include a large-scale maximum containment laboratory and a small-scale maximum containment medical evacuation and hospitalization unit [15]. With the change to a pure defensive mission in 1969, the facility was renamed the US Army Medical Research Institute of Infectious Diseases (USAMRIID) [15]. The USAMRIID has led the continued development of medical and public health countermeasures to biologic agents; all USAMRIID research is unclassified [8]. The USAMRIID has published two online detailed manuals on defense against biological and chemical warfare: (<http://chemdef.apgea.army.mil/textbook/contents.asp>) & (<http://www.usamriid.army.mil/education/bluebook.html>)

Focus on Biopreparat. After signing the 1972 Biological and Toxic Weapons Convention, the Soviet Union secretly continued their biological weapons research and development program under the aegis of a civilian biotechnology research program known as “Biopreparat” [8, 9]. During the 1970s and the 1980s the program operated a string of research laboratories and production facilities employing 55,000 people [8]. After Russia inherited the program from the Soviet Union in 1992, President Yeltsin announced that he would discontinue the program [8]. Despite this declaration, high level defectors revealed that the program continued. One of these defectors, the deputy director of Biopreparat, Ken Alibek, described an extensive secret biological weapons program in his popular book: *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program, Told from the Inside by the Man Who Ran It*. According to Alibek, Biopreparat activities included [17]:

- Multiple ‘on demand’ biological warfare production facilities for the war-time annual production of 300 to 1000 tons of anthrax and up to 100 annual tons of plague, tularemia, glanders, and brucellosis.
- ‘On demand’ biological warfare production facilities for the war-time production of smallpox, and Marburg virus.
- Research into creating a weapon out of HIV.
- Research into creating new vaccine and drug resistant varieties of conventional biological weapons.
- Research into creating new viruses with secret virulence properties and unknown countermeasures by fusing different viruses.

The preceding discussion does not mean that only the US and the USSR produced and stockpiled biological weapons. Various authorities have claimed that as many as 5 to 12 nations currently have biological weapons in their national armories [9, 11, 18].

In 1999 the CDC embarked on a congressionally mandated program to improve the national response to bioterrorism. To guide this effort, the CDC convened a panel of experts to categorize biological agents for the potential of the agent to be used as a weapon for biological terrorism [2]. To make this assignment the panel used the following four criteria [2]:

- Potential for causing massive illness and death.
- Potential for delivery to large populations.
- Potential for causing fear and civil disruption.
- Public health preparedness needs for surveillance, diagnosis, and stockpiling countermeasures (*i.e.*, vaccine and antimicrobial agents).

With these criteria in mind, the panel assigned the agents to three risk categories (A-C) [2]:

- Category A: greatest threat.
- Category B: moderate threat.
- Category C: potential to become a major threat in the future.

To signify their relative value for bioterrorism, Tables 5.1 and 5.2 also include a bracketed [A, B, or 'unranked'] designation for the CDC risk category. The tables do not include new diseases that have the potential to become threats in the future (Category C) like Nipah virus and Hantavirus.

The following paragraphs discuss in detail the six Category A agents the CDC considers the greatest threat for bioterrorism.

ANTHRAX

When authorities list infectious diseases as potential biological weapons, anthrax always seems to be at the top of the list [2, 9, 11, 18]. Indeed, there are probably more examples of the use of this agent as a biological weapon than for any other agent.

Anthrax is a large, encapsulated, Gram positive, spore-forming, bacillus, bacterium [19, 20]. Normally the microbe causes a disease of herbivores resulting in occasional epidemics in livestock [19, 21] and sporadic occupational infections of farmers, sheepherders, butchers, taxidermists, weavers, and wool handlers [21], from which the organism gets the name 'wool sorter's disease.' Anthrax is also known as 'charcoal,' 'blackbane,' and 'malignant pustule' in recognition of the pitch black 'scab' (or more formally the 'eschar') that characteristically covers the painless ulcer at the site of the skin ('cutaneous') infection [19]. Also characteristically the rim of the ulcer develops an unusual amount of swelling ('edema') [19]. Anthrax contaminated foodstuffs can also cause a gastrointestinal form of the disease with a high fatality rate (25-60%). The disease is not transmissible from person to person.

While cutaneous disease can be lethal (20% lethality in untreated patients, <1% in treated patients) [21], the fearsome reputation of the disease comes from the high fatality (80% lethality) rate that follows inhalational anthrax [21] and the low lethal inhalational dose (one millionth of a gram of spores) required to produce disease.

When spores come into contact with the host, either by direct contact, inhalation, or ingestion, the spores transform ('germinate') into a rapidly growing ('vegetative') form [19]. It is believed that germination can take place as long as 60 days after inhalation [20, 21]. The number of spores required to kill 50% of exposed individuals has been estimated to be 2000 to 55,000 spores [21, 22]. Vegetative cells produce two toxins, edema toxin and lethal toxin, killing the local tissues ('necrosis') and causing local swelling and bleeding ('hemorrhage') [19,

21, 22]. While the incubation period for gastrointestinal and cutaneous disease is relatively short (0.5 to 12 days) the incubation period for inhalational anthrax can be long. As noted in the following discussion of the Sverdlovsk incident (see below) cases occurred as late as 43 days after exposure [23]. For this reason, authorities fear that inhaled spores will survive and germinate if the antimicrobial therapy is not continued for at least 60 days [20, 21].

Inhalational anthrax begins as a biphasic nonspecific illness with fever, malaise, muscle aches and pains and a dry cough for 1-3 days [19-21]. The first phase is followed by a precipitous decline with greater fever, acute shortness of breath, sweating, and a blue discoloration of the skin due to lack of oxygen ('cyanosis') [19-21]. At this time the patient may wheeze and develop swelling of the chest and neck [19, 20]. Ultimately the patient loses consciousness, develops shock, and dies within in 1-2 days [20]. Characteristically, X-ray examination of the chest shows widening of the central structures ('mediastinum') that include the major blood vessels, airways, and lymph nodes; swelling and localized bleeding causes the widening of the mediastinum [19-21]. For the physician, this mediastinal widening in a previously healthy patient with a flu-like illness signals the diagnosis of inhalational anthrax [19, 21]. In a quarter of cases the patient also has a bloody localized pneumonia believed to mark the site of the original inhalation and implantation of the anthrax spores [20, 21].

Anthrax is diagnosed by recovering the causative organism from normally sterile body fluids and tissues [9, 20]. For epidemiological purposes of mapping exposure, microbiologists will obtain swab cultures of the nasal passages for anthrax. When positive these cultures indicate exposure, but not necessarily infection [20]. The microbiologist may also call upon a variety of molecular and antibody techniques to confirm infection, investigate outbreaks [20] and expose hoaxes [21].

With early diagnosis the illness can be cured by antimicrobial therapy. The drugs penicillin, tetracycline, and ciprofloxacin are all effective [21]. There is concern, however, that any group that would weaponize anthrax would take the additional step to make the organism resistant to multiple antibiotics (particularly penicillin and tetracycline) [20, 21] – a maneuver that can be accomplished fairly readily in the research laboratory. For this reason authorities recommend the drug ciprofloxacin as the first choice defense against anthrax in the setting of a terrorist attack [20, 21, 24].

Focus on Sverdlovsk: The 1979 accidental release of anthrax in Sverdlovsk illustrates what could happen in an anthrax attack. The drawing in Figure 5.1 is based on the report by Meselson et. al. [23] who described this outbreak. The larger drawing shows the city limits of Sverdlovsk, a city of 1.2 million located in the former USSR (now Ekaterinburg, Russia). In 1980 reports began appearing of anthrax in residents of Sverdlovsk as well as in animals to the south of the city; the triangles on the larger map mark the locations of villages that reported livestock anthrax.

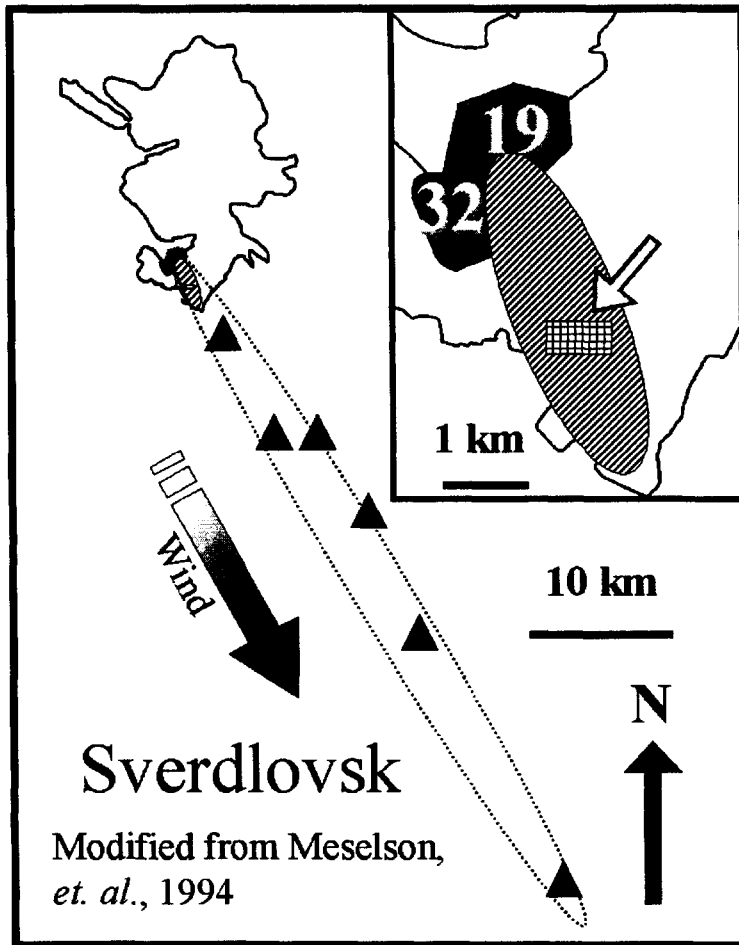


Figure 5.1 Geographic epidemiology of the 1979 anthrax outbreak in Sverdlovsk as described by Meselson *et al.* [23]. See text for details.

The investigative team examined old records and interviewed survivors and the families of victims. They counted 77 victims, 66 of whom died from their infection [23]. The outbreak began suddenly with 28 victims identified in the first week, and then tapered off with the last victims occurring in the sixth week [23]. This 'epidemic curve' characterizes a 'point source' outbreak. The team's information allowed them to map the location of 66 of the victims on April 2, 1979, the day they believed the accidental release took place. Meselson found that 57 of these 66 victims lived or worked within a narrow zone approximately 4 km long that stretched from a military facility (Compound 19) to the Sverdlovsk city limits [23]; the slashed ellipse in the insert maps this exposure zone. This zone paralleled the direction of the prevailing winds (large broken arrow) on April 2nd. Eighteen victims worked in a ceramics factory located in the middle of the exposure zone (the hatched box designated by the open arrow in the insert) [23]. The insert also shows the location of two military facilities, Compounds 19 and 32 (gray polygons); Compound 19 produced anthrax and is believed to be the source of the outbreak. To account for the geographic clustering, Meselson *et al.* postulated that an anthrax plume (dotted ellipse on the larger map) originated from Compound 19 and followed the prevailing winds. The plume stretched some 50 km downwind of Sverdlovsk and contaminated the environment, resulting in human and animal anthrax [23]. Government officials responded to the outbreak by vaccinating animals and nearly 50,000 humans [23]. Apparently since the outbreak there have been no further cases of anthrax [23].

A crude anthrax vaccine exists that provides protective immunity against cutaneous anthrax [20, 21, 25]. The material is made from a culture filtrate harvested from a noninfectious, avirulent strain of anthrax [20, 21]. Vaccination can be performed to prevent illness (prophylaxis) as well as to prevent the activation of illness after exposure (post-exposure prophylaxis) [20]. There is concern, however, that weaponized anthrax may also have been manipulated so that the vaccine would also be ineffective [21]. Controversy surrounds the vaccine concerning an unconfirmed reputation for causing troubling side effects [20] and because vaccine efficacy to prevent inhalational anthrax has not been – for understandable reasons – rigorously tested [26]. Since the vaccine has not been produced since 1998 [24] supplies are limited [20, 21]. Generally speaking the vaccine is not available to civilians [24, 25]. After the 2001 attack through the US mails (see below), the Department of Health and Human Services agreed to make the vaccine available as an investigational drug to civilians exposed to inhalational anthrax [26].

Weaponization requires fabricating the anthrax spores into particles 5-17 μ m in size by drying the material, mixing it with a powdery substance like silica, grinding the preparation into a fine powder, and treating the powder to diminish static charge [22]. Particulate matter prepared in this manner can be easily dis-

persed as an aerosol that remains aloft for a prolonged period and can be inhaled deeply into the lungs [11]. The resulting weapon has the advantage of broad dispersal from a single delivery point, but the disadvantage that the easy dispersability makes it difficult for the aggressor to limit the attack to the target population. After the material has settled, further disturbance can resuspend the dust leading to further infections ('secondary dispersal') [21].

Focus on anthrax in the US Postal Service, 2001. Just eleven days after the terrorist attack on the New York World Trade Center, cases of anthrax began appearing in the US. Initially considered coincidental, it soon became evident that someone had used the mail system to attack politicians and members of the print and broadcast media with anthrax. In addition to the targeted individuals, mail workers and uninvolved citizens also developed anthrax. Altogether some 22 individuals developed anthrax; eleven had inhalational anthrax of which five died [22, 27]. Although the investigation is incomplete, the bioterrorist apparently packaged a weaponized, antibiotic susceptible, 'Ames' strain of anthrax into mailing envelopes [22]. The weaponization strongly suggested the material was not prepared by the terrorist but came from the biological weapons stock of some unknown nation – possibly even the US [28]. Because of weaponization, the powder had great properties of dispersal, including penetration through the mailing envelope to cross-contaminate mail and contaminate mailing machinery as well as secondary dispersal leading to persistent contamination of the office buildings [22]. Although the number of casualties was relatively small, the terrorist⁴ succeeded in causing tremendous national fear and disruption of government facilities resulting in considerable cost [22].

Reportedly the Soviet Union produced 30 metric tons of anthrax and the United Nations Special Commission (UNSCOM) claims that Iraq manufactured 84,250 liters of anthrax spores [13]. In comparison, different authorities have reported that the release of 50 kg of anthrax over an urban population of 5 million would cause 100,000 deaths and 250,000 casualties [21] and the release of 100 kg over Washington D.C. would cause 130,000 to 3,000,000 deaths [21].

⁴ This incident may actually represent a crime committed with a biological weapon or 'biocrime' rather than 'bioterrorism' *per se*. Authorities speculate that the perpetrator is an American microbiologist connected to the American biological weapons program, who inadvertently caused casualties in a misplaced attempt to draw attention to the weapons program or lack of funding for bioterrorism [28]. These authorities suspect the casualties were accidental because the perpetrator had sealed the envelopes with tape and urged the recipient to take antibiotics for anthrax exposure [28]. These precautions suggest that the perpetrator did not realize that the envelope was not impervious to anthrax but actually had pores large enough to allow the anthrax spores to penetrate the paper and spread throughout the surroundings [28].

The high fatality rate, rapid clinical pace, and limited countermeasures make this a fearsome illness, therefore a great weapon from the viewpoint of the terrorist. The capacity to spread the material by aerosols enables the terrorists to attack large numbers of people providing the terrorist has access to military grade material. Because of the infrastructure required to produce weapons grade material, it is unlikely that weaponized anthrax can be obtained from any source other than a nation-state [21]. The terrorists contemplating an attack with anthrax will either have to steal the material, solicit a gift, or prepare it themselves. Terrorist manufactured anthrax will probably not have the dispersability and infectivity of weapons grade material, although it could still represent a potent weapon [4].

SMALLPOX

The last reported case of wild smallpox occurred in Somalia in 1977 [29]. In 1980 the General Assembly of the World Health Organization declared smallpox extinct [29] and recommended that all remaining stocks of the virus be transferred to secure laboratories in either the US or the USSR [30]. Despite calls for the destruction of these residual stocks, the organism remains in the US and Russia [30]. Reportedly the USSR biological weapons program produced 20 metric tons of this material [9].

The organism is a DNA virus of the Orthopoxvirus family that includes monkeypox, vaccinia, and cowpox [30]. Two types of smallpox exist: the virulent Variola major (with a case fatality rate of 30%) and the less virulent Variola minor (or alastrim) (with a case fatality rate of 1% or less) [30]. The infectious dose is unknown but believed to be only a few viral particles ('virions') [30]. Infection begins with implantation of the virus on the oropharyngeal and respiratory mucosa, from there it migrates to regional lymph nodes where it multiplies [30]. Three to four days after exposure smallpox enters the bloodstream ('viremia') and spreads to the spleen, bone marrow, and lymph nodes [29]. A secondary cycle of viremia occurs on day eight resulting in fever and toxemia. The incubation period is 12-14 days; the illness begins with a two-to-four day prodrome of high fever, malaise, prostration, headache and backache [29]. In some 30% of patients the natural immune response leads to a severe toxic reaction that ends in death [29].

The characteristic feature of the illness is a skin rash ('exanthem') that begins as small red bumps ('papules') that over time fill with clear fluid to become 'vesicles' [29]. The vesicles then fill with pus ('pustules') and break open leaving a crusted ulcer, known as the 'pox,' that heals with a deep pit [30]. The onset of the exanthem heralds greatest communicability [30], but communicability at this time is through the saliva [30]. Prior to onset of the exanthem and during the first week of illness, a similar rash – known as an 'enanthem' – develops on the inner lining ('mucosa') of the mouth and throat. As mucosal lesions form they quickly ulcerate releasing infective virus [22]. At first, when the saliva contains relatively small numbers of virions, communicability is limited to contaminated eating and drinking utensils [22]. As the number of oral lesions increases, the number of virions in

the saliva increases, increasing communicability and reaching a maximum just prior to the onset of the exanthem [22]. At this time smallpox can be transmitted through close contact by aerosolized saliva [22]. When the exanthem appears, the vesicles rupture and release fluid containing infective virions. The virion-laden vesicular fluid soils clothing and bedding, which can in turn transmit the illness [22]. The virus is also present in large numbers in the blood clot or scab covering the pox, but the encasing fibrin network of the clot makes the scabs noninfective [30].

The illness is diagnosed by the characteristic rash, confirmed by electron microscopic examination of the vesicular fluid, and reconfirmed by propagating the organism on tissue culture and verifying the genetic identity by molecular techniques [30]. Needless to say, such analysis must be conducted in high-containment laboratories [30].

Aside from supportive nursing care, there is no therapy for smallpox [24, 30]. In an unimmunized population, 10 to 20 secondary cases occur for every primary case [30]. The public health response depends entirely on identification and isolation of the infected patients followed by contacting and immunizing all people exposed to the patient.

Smallpox can be prevented by vaccination; the worldwide vaccination program led to the illness becoming extinct. With eradication of smallpox from the US, the medical necessity for immunization ceased, so routine vaccination stopped after 1972 [30]. Smallpox vaccination does not lead to life-long immunity, so with cessation of vaccination, immunity to smallpox has waned; authorities believe that at this time, regardless of past immunization, virtually all Americans are susceptible to smallpox [30]. The CDC has between 7 to 15 million doses of the old vaccine [24, 25]; this would not be enough to protect against repeated smallpox attacks or a broad-based multi-locality attack [30]. Studies in progress suggest that this vaccine stock could be diluted to extend the coverage to five to 10 times as many people [31]. In the meantime the US is seeking to reestablish a vaccine manufacturing program that could expand the available supply [25].

Focus on Smallpox in New York City, 1947. The 1947 New York outbreak of smallpox serves as an encouraging example of an effective public health response to an unrecognized outbreak of smallpox in an unvaccinated US population [22, 32]. In 1947 a US citizen, the 'index' case, journeyed to Mexico where he acquired smallpox [32]. Shortly after returning to New York City, he developed a severe but atypical form of smallpox that resulted in hospitalization and later his death, the first death in New York City due to smallpox since 1939 [32]. The index patient's physicians failed to make the diagnosis until two typical secondary cases of smallpox appeared [32]. Public health officials responded to the outbreak by isolating the 'index' patient, secondarily infected patients, and vaccinating a potentially exposed population of 6.3 million [32]. By these measures they limited the outbreak to three deaths and twelve cases [32].

The high lethality, gruesome death, and likelihood for secondary spread make this a truly fearsome disease, perhaps the most fearsome agent for bioterrorism. Fortunately the disease is extinct and the remaining stocks of the organism are controlled by only two countries, the US and Russia (inheritors of the USSR weapons program). Unfortunately, the collapse of the Soviet economic and political structure in the 1990s has raised concerns that the Russian government may have lost control of the inherited smallpox inventory [18, 9]. The Soviets reputedly produced 20 metric tons [9] of smallpox in weapon form, making it possible that some stocks have fallen into the hands of terrorists or countries that support terrorism. Reputedly both Iraq and North Korea now have weapon stocks of smallpox [33]. If the agent could be procured for bioterrorism, presumably a terrorist organization would hesitate to re-release an incurable, highly infectious, extinct disease. Aside from the universal condemnation such an act would incur, it would also expose the members of the organization as well as their supporters to dying of smallpox themselves.

TULAREMIA

The '*tularensis*' of *Francisella tularensis* comes from Tulare County, California where the organism was first discovered to produce a plague-like illness in rodents [34]. The '*Francisella*' honors Dr. Edward Francis who discovered that the deer fly transmitted the microbe to humans causing an illness previously known as deer fly fever but now known as 'tularemia' [34]. Originally considered a North American disease, the organism has subsequently been recognized as the cause of large outbreaks in Europe and the former USSR [34, 35].

The microbe is a small non-motile, aerobic, Gram negative, coccobacillus, bacterium [35]. The organism exists in two subspecies forms or 'biovars,' the more virulent 'biovar tularensis' (type A) is native to North America and the milder 'biovar palaeartica' (type B) is native to Europe and Asia [34, 35]. The bacterium normally lives and multiplies in small mammals (voles, mice, rats, squirrels, rabbits, and hares) that serve as the natural 'reservoir' of infection [34, 35]. The animals acquire the illness through arthropod (ticks, biting flies, mosquitoes) bites and by contact with a contaminated environment [35]. Most humans become infected by the bite of a tick or a fly, but the illness can also be acquired by handling infected animal tissues, consuming contaminated soil, water, meat, or vegetation, and from inhaling aerosols [34, 35]. The microbe is highly infectious; it is believed that as little as ten organisms can cause disease [34]. Unless they take precautions, laboratory workers have a substantial risk of accidentally infecting themselves through direct contact or inhalation of an aerosol [35]. Fortunately, there is no human-to-human transmission [34, 35].

The disease exists in six clinical forms that vary according to the body site that first comes in contact with the microbe, the virulence of the organism, and the number of infecting organisms [35]. The most common forms of the illness begin

with the bite of an arthropod or contamination of a break in the skin; from this 'portal of entry' the organism spreads to local lymph nodes, producing painful enlargement (glandular tularemia) [35]. Usually, however, the organism also multiplies at the portal of entry resulting in one or more papules that rupture and ulcerate (ulceroglandular) [35]. If the portal of entry is the lining of the eye, the disease is known as 'oculoglandular' [35]. If the organism infects the throat through consumption of contaminated food or water it is known as 'oropharyngeal' [35]. Inhalation of the organism (as well as secondary spread from another site of infection to the lung) produces a severe lung infection known as 'pneumonic' tularemia [34, 35]. Sometimes the organism does not produce a local infection, but instead causes a generalized severe form of disease known as 'typhoidal' tularemia that can include clinical features of pneumonic tularemia [35].

A panel of experts, known as the 'Working Group on Civilian Biodefense' (WGCB) reviewed the utility of tularemia as a biological weapon and postulated that an attack would most likely come in the form of an aerosol resulting in pneumonic tularemia [35]. Based on their review of the literature [35], the WGCB predicts such an attack would begin with the sudden appearance of large numbers of sick patients within 3-5 days of exposure to the aerosol, with some cases occurring as late as two weeks after exposure [35]. The patients would present with pneumonia, remarkable only in terms of the large numbers of patients presenting at the same time [35]. Patients would complain of an abrupt onset of fever, headache, chills, generalized body aches, sore throat, cough, shortness of breath, and chest pain [35]. Chest X-ray evidence of pneumonia would be present in most patients, but delayed in one-quarter to one-half of the patients [35]. Significant impairment may occur despite therapy, surviving untreated patients may experience illness lasting weeks to months [35]. Depending upon the public health response, susceptibility to antimicrobial therapy, and virulence of the weapon, fatality rates could reach 30-60%, but might be less than 2% [35]. It is possible, however, that in the event of an attack the virulence of tularemia could have been enhanced by laboratory manipulation [35].

Normally the infection can be treated with antimicrobial therapy; regimens employing a daily injection of an aminoglycoside are preferred over oral therapy with doxycycline or ciprofloxacin [34, 35]. The utility of antimicrobial therapy in the event of an attack is questionable. The organism has been engineered to be resistant to chloramphenicol and tetracycline [35] and both the US and USSR have created biological weapons using aminoglycoside-resistant strains [35]. Nevertheless, in the event of a massive attack the WGCB recommends either oral doxycycline or ciprofloxacin [35]. A small supply of vaccine exists [24], but it exhibits variable capacity to protect against inhalational disease [35] and it is not for post-exposure protection [24].

The WGCB speculated that an attack with tularemia could be distinguished from an anthrax attack by the more toxic clinical appearance of inhalational anthrax along with the telltale mediastinal widening exhibited by anthrax [35]. The attack could also be distinguished from an attack with plague by the more virulent

clinical course presented by pneumonic plague (see below) [35]. The WGCB anticipates that standard bacteriologic laboratory procedures would lead to the quick identification of infections due to anthrax or plague [35]. Unfortunately since routine procedures do not detect tularemia, the organism could escape identification until a physician requested specific testing [35].

Authorities have projected that the dispersal of 50 kg of tularemia over an urban population of 5 million would result in 250,000 casualties and 19,000 deaths [35].

PLAGUE

Synonymous with epidemic deadly contagion, 'plague' has great potential to evoke terror as a weapon of bioterrorism. The disease earned its fearsome reputation by causing three deadly pandemics in the 6th, 14th, and 20th centuries [12, 36]. The cause of plague, *Yersinia pestis*, is a Gram negative, cocco-bacillus, bacterium that demonstrates a characteristic bipolar (safety pin) staining under the microscope [12, 36]. The genus name honors Alexandre Yersin who in 1894 discovered the etiology of plague in Hong Kong at the beginning of the third and most recent pandemic [12].

Plague is endemic to Europe and Asia; authorities suspect it spread to North America during the most recent pandemic by causing epidemic ('epizootic') infection in North American rodents [12]. The disease normally resides in rodents, where it is transmitted from one animal to the next by the bite of a flea (the 'vector' of transmission) [12, 36]. One bite can transmit as many as 24,000 organisms [12], but it is estimated that only one to ten organisms are required to infect a person [12]. The oriental rat flea is the classic vector [12] but all kinds of fleas can transmit the illness [12]. When the animal host dies of the disease, the flea leaves the dead host and seeks a new live host [36]. Normally the rodent population both maintains and contains the disease; humans experience only sporadic 'wild' disease acquired by handling infected tissues or by the occasional fleabite from a rural rodent flea [12]. When massive numbers of infected urban rats die, such as in epizootic infection, the fleas may leave their customary rodent hosts in large numbers to infest human hosts causing an urban outbreak of plague [36]. The urban outbreak can expand to become an epidemic if the disease spreads to the lungs of infected humans ('pneumonic plague'), who in turn transmit the disease through the air by coughing [12, 36]. Inhalation of respiratory secretions is the only way epidemic disease can spread from human-to-human [36].

Most (85%-90%) patients with wild disease have 'bubonic plague' [12] that begins when a fleabite introduces the microbes into the skin, whereupon the organisms transform and begin to produce disease-causing toxins and virulence factors [12]. These factors enable the germs to migrate to the local lymph nodes, where despite the host's defensive mechanisms the organisms multiply, causing local inflammation and tissue destruction [36]. The patient perceives the illness at this time as the abrupt onset of high fever, chills, fatigue, headache, nausea and

vomiting, followed by painful swelling of the lymph nodes near the fleabite [12]. The term 'bubonic plague' derives from the characteristic swollen lymph nodes, known as 'bubos,' that arise one-to-eight days after the fleabite [12, 36].

In a minority of wild cases (10-15%) the fleabite leads to direct invasion of the blood stream by the *Y. pestis* bacilli producing 'septicemic plague' [12]. More commonly (23%) the microbes enter the bloodstream after multiplying in the local lymph nodes leading to the combination of bubonic and septicemic plague [12]. Septicemia generates an intense generalized inflammatory response ('sepsis'), that can result in shock, multi-organ failure, bleeding into the tissues ('purpura'), impaired blood clotting ('disseminated intravascular coagulation' – 'DIC'), impaired breathing ('respiratory distress syndrome'), and gangrene of the extremities [12, 36]. The extremity gangrene turns the limbs black, from which the disease gets the name the 'black death' [36]. Septicemic plague has a mortality of 50% if untreated [36].

Once the microbes enter the bloodstream they can migrate to other sites, such as the lungs causing pneumonia [36]. Very few (1%) patients with wild disease present with only pneumonic plague [12], more often (9%) they present with both bubonic and pneumonic plague [12]. Patients have cough, chest pain, shortness of breath, and a productive sputum [12, 36]. The chest X-ray shows a lobar pneumonia [36]. Pneumonic plague has a mortality of 100% in untreated patients [36] and 15% in treated patients. Pneumonic plague acquired from another human has a higher mortality than wild type disease because the victim has inhaled organisms that have already undergone transformation into the virulent form by growing in another human victim [12].

Normally physicians diagnose the infection by recovering the organism from the bubo, blood, or sputum by using standard bacteriologic methods [9, 12, 36]. The infection can be confirmed by detecting tularemia antibodies ('serologic assay'), but this is helpful only for retrospective confirmation as it takes time for the patient to develop an immune response [12, 36]. Rapid molecular techniques exist to confirm the identity of the organism [12] but these are only available through public health, military, and CDC laboratories [36].

To avoid further transmission, infected patients require strict isolation; for the first four days of therapy for 'pneumonic' plague (as well as for a wound draining *Y. pestis*) and for the first 48 hours for all other infections [12]. Therapy is best accomplished with injectable antibiotics (gentamicin) for a minimum of 10 days [12, 36]. In cases of mild infections or in situations where injectable antibiotics are not feasible, the patient can be treated with either oral doxycycline (or tetracycline) or ciprofloxacin [12,36]. Exposed patients can be protected from acquiring the disease by the preventive ('prophylactic') post-exposure oral administration of either doxycycline or ciprofloxacin for seven days [12, 36].

A US-licensed, formaldehyde-killed, whole-cell vaccine exists, but the vaccine is reserved for military use and patients with occupational exposure [12]. The vaccine may not be effective against pneumonic plague [12] and it is no longer readily available, having been discontinued by the manufacturer in 1999 [24, 36].

Japan, the US, and the USSR examined the utility of plague as a biological weapon [8,36]. While it is possible, that like Japan [8] an attacker would use fleas, the result would be the less deadly bubonic plague and would also require sophisticated technology to maintain, infect, harvest, and package such a flea weapon [12]. Instead, experts predict that a plague attack would use aerosolized bacteria causing large numbers of infectious pneumonic plague [12, 36]. In 1970, the WHO reported that the discharge of 50kg of plague over a city of 5,000,000 would cause 150,000 cases of pneumonic plague with 36,000 deaths [36]. Experts project that human illness would begin in 1-6 days post attack [36] and death would occur in 2-6 days [36]. A plague attack should become evident by the abrupt presentation of large numbers of people with the pneumonic form in an atypical area for plague [36] and without the typical die-off of urban rodents that occurs before human outbreaks [36].

VIRAL HEMORRHAGIC FEVERS

In his novel *Executive Orders*, the popular writer Tom Clancy described a fictional bioterrorist attack on the US by an imaginary country the "United Islamic Republic." In this story the attacker used spray cans filled with Ebola virus to create an infectious aerosol and expose people attending trade shows. Although Tom Clancy's story included the deaths of several thousand Americans due to Ebola virus, the fictional attack ultimately failed to cause the intended horrific epidemic of hundreds-of-thousands to millions of deaths. The attack failed because the virus failed to cause human-to-human transmission ('secondary cases') and the telltale clinical features of Ebola virus quickly alerted physicians to the outbreak. Informed of the outbreak, public health officials rapidly instituted strict but effective controls to contain and prevent further spread of the illness. Although entirely imaginary, this story underlines the weaknesses and successes of such an attack. Even though the enemy successfully collected and propagated the deadly virus, the project required an expensive program to find, contain, and weaponize the organism. Even though the enemy succeeded in surreptitiously attacking US citizens, causing many deaths and tremendous terror, the outbreak failed to spread because biologic barriers and public health barriers interrupted the human-to-human transmission.

Despite Mr. Clancy's optimistic yarn, viral hemorrhagic fevers (HF) pose a serious and credible threat for a successful terrorist attack. Unlike smallpox, these deadly viruses exist in the wild where they can be collected. For example in 1993 the Aum Shinrikyo religious cult sent a group of 16 cult doctors and nurses to Zaire disguised as a medical mission with the purpose of bringing back samples of Ebola virus for weaponization [14]. Many of the HF organisms can be propagated and harvested from tissue culture in sufficient quantities to prepare infectious materials [37]. Blood harvested from infected patients is highly contagious, but requires direct contact to transmit illness. Unlike anthrax, botulinum, plague, and tularemia, bioterrorists could use this agent without having to first weaponize the

organisms and construct a weapon production facility. All that would be required would be for a group of suicidal terrorists to willingly expose themselves to the wild agent and then move through population centers as their illness progressed. While such an act would probably not cause many secondary cases, it would cause terror and prompt a massive public health response.

Viral HF refers to a disparate group of organisms (see Table 5.3) that share common clinical and microbiologic features [37]. HF viruses are simple RNA viruses with lipid envelopes [37]. The virions are susceptible to detergents, acids, and household bleach, but they are stable at neutral pH particularly in the presence of protein [37]. As a consequence of the protein-enhanced stability, infectious virions are stable in blood and tissue for prolonged periods of time [37]. Virions are also stable as small particle aerosols making it possible to 'weaponize' these viruses [37].

Table 5.3 Hemorrhagic fever (HF) viruses [37].

Hemorrhagic Fevers (HF)			
<i>Arenaviridae</i>	<i>Bunyaviridae</i>	<i>Filoviridae</i>	<i>Flaviviridae</i>
Lassa fever	Rift Valley fever	Marburg virus	Yellow fever
Argentine HF	Crimean-Congo HF	Ebola virus	Dengue
Bolivian HF	Hantavirus		Kyasanur-Forest
Brazilian HF	Korean HF		Omsk HF
Venezuelan HF			

The pathologic process underlying viral HF is damage to the micro-circulatory ('vascular') system resulting in the movement of fluids from the blood into the tissues [37]. The loss of circulating blood volume generates profound shock while the vascular damage and blood clotting abnormalities lead to characteristic bleeding ('hemorrhage') into the tissues [37]. As a group HF viruses exhibit a high morbidity and mortality [37] with death rates ranging from 5% to 25% or higher [37, 38]. Ebola virus outbreaks have had mortality rates as high as 50-90% [37, 38].

While the precise mix and degree of clinical features varies with the particular illness⁵, certain features are common to most HF syndromes [37]. Patients

⁵ Unlike the other HF illnesses, the *sin nombre* Hantavirus produces a syndrome characterized by pulmonary edema [37]. Lassa fever patients do not typically develop hemorrhages and hemorrhage is seen in only severe cases of Rift Valley fever [37]. Liver failure is characteristic of Yellow fever and is seen in a small proportion of patients with Crimean-Congo HF, Rift Valley fever, Marburg HF, and Ebola HF [37].

usually present with fever, muscle aches ('myalgia'), and exhaustion ('prostration') [37]. They may also have headache, sore throat, abdominal pain, and diarrhea [38]. Characteristically the physical examination reveals a low blood pressure ('hypotension'), flushing, and point-like bleeding into the tissues ('petechiae') [37]. The hypotension progresses to shock and kidney failure [37]. In nearly all syndromes the blood cells that normally promote clotting decrease to a varying degree (*i.e.* 'a low platelet count') resulting in bleeding tendencies (DIC) [37]. As a consequence many HF patients develop spontaneous hemorrhages particularly from mucosal surfaces and traumatic injuries (*e.g.* skin puncture sites for blood samples and administration of intravenous fluids) [37]. Involvement of the liver is also common and there may be involvement of the nervous system and the lungs [37].

Of the HF viruses only Lassa fever, Marburg virus, Ebola virus, and Crimean-Congo virus have caused significant outbreaks with person-to-person transmission [38]. Transmission occurs by close personal contact and contact with infected tissue, blood, secretions, and excretions [38]. There is no convincing evidence of transmission through the air [38]. As the outbreak progresses, transmission efficiency from case to case becomes increasingly inefficient, so outbreaks tend to quickly dissipate [38].

The HF viruses infrequently infect humans [37]. For most HF viruses wild animals, particularly wild rodents, serve as the reservoir of infection [37]. Humans acquire the diseases from close contact with infected animals (*e.g.*, slaughtering and consumption) or by the bite of an arthropod vector (*e.g.*, mosquitos and ticks) [37]. Because HF are closely linked to reservoir animals and transmitting vectors, the HF viruses are geographically restricted [37]. A travel history to rural sites in an endemic region is a major clue to the etiology of HF [37, 38]; on the other hand travel restricted to urban sites in an endemic region makes the diagnosis unlikely [38]. Bioterrorism should be suspected when large numbers of victims suddenly appear outside of the normal geographic locality for the HF [37].

The major alternative diagnostic considerations for HF are malaria and sepsis, since these two conditions can present with clinical features similar to HF [37, 38]. The presence of malaria can be determined by examining blood smears while sepsis can be determined by isolating bacteria from the blood [38]. Laboratory diagnosis of HF can be difficult as the diagnosis is beyond the capability of community laboratories. In most cases viremia is present on admission and can be detected in the serum or plasma by sending the specimen to a public health laboratory or the CDC or the USAMRIID [37]. Blood is infectious and hazardous [37]; since many HF patients develop copious bleeding, HF patients pose a major hazard to care givers [37]. If a physician suspects HF the patient should be isolated and the physician should immediately notify local and state health departments as well as the CDC [38].

In most cases therapy for HF is limited to symptomatic support [37], however patients do not respond well to fluid support and are prone to develop pulmonary edema [37]. Ribavirin reduces Lassa fever mortality [37] and is recom-

mended for Congo-Crimean HF and severe cases of Venezuelan HF, Korean HF, Brazilian HF, Argentine HF, and Bolivian HF viral infections [39]. Acutely infected patients with Argentine HF and Bolivian HF will improve with the administration of antibodies recovered from convalescent patients [37] but this therapy is not available for other HF [37]. With the exception of the Yellow fever vaccine, there are no readily available vaccines with demonstrated efficacy [37, 39].

BOTULISM

Known as agent X before the poison had been purified and analyzed [40], botulinum toxin is the most toxic naturally occurring substance known to man [40, 41]. Botulinum toxin is also one of the first agents to be exploited as a biological weapon in the modern era [40]. For example, some historians believe that in the spring of 1942 the British used a modified hand grenade containing botulinum toxin to assassinate Reinhard Heydrich, the head of the German Gestapo and Security Service [40]. After the 1991 Gulf War, Iraq admitted to producing enough botulinum toxin to wipe out the entire world population three times over [41]. Fortunately, even though Iraq deployed missiles and bombs containing more than half of their stock of toxin, the Iraqis did not use these weapons [41]. In addition to Iraq, Iran, North Korea, and Syria are believed to have developed or are developing botulinum toxin as a weapon [41].

Immense toxicity apparently does not necessarily equal immense destructive power; on at least three occasions during the 1990s Aum Shinrikyo attacked Japanese and US military sites with aerosolized botulinum toxin but failed to cause disease [41]. In contrast to destructive purposes, highly diluted botulinum toxin has been licensed for the treatment of chronic muscle spasms that distort eye movement ('strabismus'), cause spasmodic winking ('blepharospasm'), and cause chronic neck pain and distortion of head positioning ('cervical torticollis') [41]⁶.

The bacterium *Clostridium botulinum*, a spore forming, Gram positive rod that does not tolerate oxygen ('obligate anaerobe') produces botulinum toxin [41]. While *C. botulinum* can be purchased from commercial sources, like the American Type Culture Collection, the organism can also be easily recovered from the soil [40, 41]. For example, the Aum Shinrikyo cult isolated their strain of *C. botulinum* from northern Japanese soil [41].

'Botulism' – poisoning by botulinum toxin – appears to be a disease of modern technology [40]. The disease was not readily apparent to medical historians before the introduction of new food preservation methods in the 19th century [40]. Since the hardy *C. botulinum* spores tolerate boiling, the spores contaminating foodstuffs can persist when the food is improperly cooked or preserved. If the preservation creates an environment devoid of oxygen, such as occurs in canning,

⁶ Therapeutic botulinum toxin (Myobloc® or Botox®) will not work as a weapon because each drug vial contains only a small fraction of the estimated human lethal dose.

the spores can germinate releasing the toxin [41]. Because the toxin is odorless and tasteless [41], the consumer of the tainted food may not recognize that the food has spoiled. Intoxication, however, can still be avoided by cooking the tainted food, since heating the toxin at 85°C for at least five minutes readily destroys the toxin [24, 41].

Although seven botulinum toxins (types A to G) have been described, only four have been identified with human disease (toxin A, 54%; toxin E, 27%; toxin B, 15%; & toxin F, 2% of cases respectively) [41]. The remaining three types (C, D, & G) are known from non-human sources, although these types appear to be equally toxic to humans and have been reported to cause rare human cases [41]. Of interest, type A is most commonly found in the western US, type B in the eastern US, and type E in Canada & Alaska [40, 41]. Toxin typing is important for prescribing the correct neutralizing antitoxin and for epidemiological analysis [41].

Neurotoxins like botulinum toxin and the plant toxin curare cause paralysis by blocking the transmission of signals across the microscopic gap ('synapse') between the nerve cell and the associated muscle cell ('neuromuscular junction'). Normally, the nerve cell signals the muscle cell to contract by first forming a small bud ('synaptic vesicle') on the nerve cell surface that contains the chemical ('neurotransmitter') acetylcholine. The vesicle pinches off the nerve cell, crosses the synapse and then binds and fuses to the muscle cell releasing the acetylcholine into the muscle cell [41]. The released acetylcholine causes muscle contraction by binding to a specific acetylcholine receptor on the muscle fiber [41].

On a weight-by-weight basis, botulinum toxin is a far more potent toxin than other toxins like curare. Curare blocks neurotransmission by binding to the acetylcholine receptor, physically preventing acetylcholine from binding to the receptor [40, 41]. Botulinum toxin, however, multiplies its effect by repeatedly catalyzing the destruction of proteins required to release acetylcholine into the muscle cell [40, 41]. Specifically, botulinum toxin is a zinc-dependent metallo-proteinase that enters the nerve cell and cleaves specific proteins that are normally required to promote the fusion of the synaptic vesicle containing acetylcholine with the muscle cell [40, 41]. This blocked fusion prevents release of the acetylcholine into the nerve cell resulting in an uncontracted ('flaccid') muscle paralysis [40, 41].

Botulism occurs in three natural forms (food-borne, wound, and intestinal) that rely upon absorption of the toxin across a mucosal (or wound) surface into the blood [41]. The toxin does not penetrate intact skin, so contact botulism does not occur; however, inhalation of aerosolized toxin has occurred as a laboratory accident [40, 41] and is the most likely route of administration for a bioterrorism attack [40, 41].

Botulism characteristically presents with paralysis of the head and neck muscles that progresses to involve all of the skeletal muscles in a patient with normal mental function and no evidence of acute infection such as fever [41]. Depending on the amount of toxin, the extent and pace of paralysis varies from patient to patient [41]. The illness usually begins 12 to 72 hours after ingestion of

tainted food [40, 41] when the patient begins to drool and experience difficulty chewing, speaking, swallowing, and seeing [41]. The paralysis spreads equally to both of the upper limbs, followed by the trunk and then both lower limbs [41]. The paralysis can be severe enough to require mechanical breathing support [40, 41]. On physical examination the physician finds drooping of both eyelids, enlarged and slowly reacting pupils, loss of the gag reflex, inability to hold the head upright, weakness, and diminished deep tendon reflexes [41]. If the patient has food poisoning, the patient may also complain of abdominal pain, nausea, vomiting, and diarrhea. These gastrointestinal symptoms appear to be due to other bacterial products in the spoiled food rather than to the botulinum toxin *per se* [41]. Because recuperation requires regeneration of the neuromuscular junctions, recovery may take weeks to months during which time the patient may require extensive nursing care and mechanical breathing support [41].

Intestinal botulism occurs primarily in infants and presents with constipation, wound botulism occurs with contaminated injuries and has a similar presentation to food-borne botulism except the patient may have a fever due to wound infection [41]. Neither condition is likely to be the result of a bioterrorism attack [41]. A bioterrorism attack could occur through contamination of one or more food products, but this would be an inefficient use of the poison. Botulism is not known to be acquired by contaminated water [41] and this is an unlikely attack method because water purification treatments inactivate the toxin and because poisoning a major water source like a reservoir would require an exceedingly large amount of toxin [41].

On the other hand, experts have projected that in an urban setting aerosolization of a single gram of toxin could kill more than 1 million people [41]. Although inhalational botulism does not occur in nature, animal experiments and a German laboratory accident in 1962 involving three workers, indicate that inhalational botulism will appear similar in all respects to food-borne botulism [40, 41]. Regardless of how it is acquired, botulism is not contagious because it is an intoxication rather than an infection [41].

Physicians may misdiagnose the sporadic case of botulism, but the diagnosis becomes increasingly evident as groups of patients present who share common features of geography, time, and exposure [41]. The diagnosis is confirmed by a 'mouse bioassay,' meaning the laboratory injects a mouse with a test fluid to determine if the fluid will produce signs of botulism in the mouse. If the animal displays symptoms, then the laboratory confirms the presence of the toxin by adding an antiserum to the fluid to nullify the toxin. The fluid sample could be a sample of the patient's serum or a filtrate of a clinical sample (such as vomitus, stool, or gastric contents) or a filtrate of a suspect food [40]. This assay can detect as little as 0.03 nanogram⁷ (ng) of botulinum toxin and generates a result in one to two

⁷ In contrast the estimated lethal dose for injected toxin is 0.09-0.15 µg, for inhaled toxin is 0.70-0.90 µg, and for ingested toxin is 70 µg [41].

days [41]. The assay must be performed before the patient receives antiserum therapy and is available only through select public health laboratories [41]. The assay will not only confirm the diagnosis of botulism but also reveal the toxin type. Finding large numbers of patients with an unusual type of botulism (*e.g.* A or B from the wrong region or type C, D, F, & G) should prompt the consideration of a terrorist attack [41].

If diagnosed quickly, disease progression can be prevented by administration of the correct antiserum. Horse antiserum to botulinum toxins A, B, & E is available from the CDC [24]. Recipients may develop allergic reactions to the horse serum including shock ('anaphylaxis'), hives ('urticaria'), and a generalized inflammatory condition known as 'serum sickness' [24, 41]. A new antiserum against all seven types of botulinum toxin is under investigation by the US Army; this antiserum has been treated to reduce the likelihood of an allergic reaction [24]. Once established there is no antidote or therapy for botulinum toxin. With supportive care, often including intravenous feedings and mechanical ventilation, the patient will recover over a period of weeks to months. Because such patients often require prolonged intensive care, authorities fear that a concerted bioterrorism attack with botulinum toxin will quickly overwhelm medical facilities [41].

An investigational pentavalent (ABCDE) botulinum toxoid can be obtained from the CDC to protect high-risk laboratory workers and military personnel [24]. The toxoid, however, does not work after exposure to botulinum toxin [24].

FUTURE PERSPECTIVES

While the weapons bioterrorists could use are fearsome, the weapons bioterrorists have used have been ineffectual and the incidents of bioterrorism have been rare.

Writing on behalf of the Monterey Institute of International Studies in a 1999 issue of *Emerging Infectious Diseases* devoted to Bioterrorism, Tucker reported that the Center had compiled an open source database of all publicly known cases where terrorists sought to use or acquire biological agents. The Monterey Institute recorded only 55 bioterrorist events over the 40-year period from 1960 through 1999, most of which were hoaxes [1]. Tucker notes that over this 40 year period only one bioterrorist attack led to casualties: the Oregon Rajneeshee religious cult caused 751 cases of food poisoning – but no deaths – in their unsuccessful attempt to manipulate local elections [1]. The only other serious incidents during this period also involved a religious cult and also proved ineffectual. The Japanese Aum Shinrikyo cult used botulinum toxin in 1990 and 1993 and anthrax in 1993 to unsuccessfully attack both the Japanese citizenry and the Japanese government [14].

In 1999 Dr. Donald Henderson⁸, who led the World Health Organization's global smallpox eradication program, commented on the paradox between the potency of bioterrorist weapons and the impotency of bioterrorism. Henderson noted four 'academic' explanations for this anomaly [18]:

- Because biological weapons have not been successfully used in the past they will not be successfully used in the future.
- Because the use of biological weapons is repugnant, no one will use them.
- The technology of bioterrorism is beyond the reach of the bioterrorist.
- The capacity of biological weapons for causing mass destruction makes the use of these weapons unthinkable.

Dr. Henderson questioned these arguments noting that technological advances, the increasing boldness of terrorists, and the willingness of nations that support terrorism (like Iraq) to produce and deploy biological weapons, predicted future disasters [18]. Considering the subsequent 2001 anthrax attack through the US mails, some might consider Dr. Henderson's warnings prophetic. Since the anthrax attack actually resulted in only 22 casualties and 5 deaths, others might consider Dr. Henderson's warnings exaggerated. To which others might reply that only a prompt massive public health effort succeeded in limiting the 2001 anthrax attack to just 22 casualties.

Perhaps the best approach is to expect that bioterrorism will never lead to massive loss of life and health but still prepare for disaster.

In preparing for disaster we are fortunate that the Internet provides ready access to updated information. Appendix 5.1 lists Internet resources on bioterrorism.

⁸ In November 2001 Dr. Henderson was appointed to direct the newly created Office of Public Health Preparedness at the Department of Health and Human Services.

APPENDIX 5.1 ELECTRONIC RESOURCES FOR BIOTERRORISM**Educational**

1. www.bioterrorism.uab.edu Agency for Healthcare Research and Quality (AHRQ): teaches physicians and nurses how to diagnose and treat rare infections and exposures to bioterrorist agents such as anthrax and smallpox.
2. www.btresponse.org American Academy of Family Physicians: contains in-depth information on recognizing, diagnosing, and treating conditions resulting from chemical and biological warfare agents.
3. www.annualreviews.org/biohazards Website of Annual Reviews provides access to online documents about bioterrorism.
4. www.aamc.org/bioferrorism Association of American Medical Colleges: teaches physicians, residents, and medical students on how to mount an effective response to terrorist acts involving biological organisms, chemical agents, and radioactive and nuclear weapons.
5. www.cdc.gov/ncidod/eid/vol5no4/pdf/v5n4.pdf Electronic issue of the journal *Emerging Infectious Diseases* devoted to the topic of bioterrorism.
6. www.idsociety.org Infectious Diseases Society of America home page: links to multiple informational and educational resources.
7. www.niaid.nih.gov/publications/bioterrorism.htm National Institute of Allergy and Infectious Disease Bioterrorism website describes NAID sponsored research and provides access to online articles.
8. www.nbc-med.org/others NBC-Med: provides electronic access to broadcasts, news reports, and training and educational resources concerning bioterrorism.
9. www.ph.ucla.edu/epi/bioter/bioterrorism.html University of California Los Angeles: general educational information in support of academic studies on the epidemiology and public health response to bioterrorism.

Response guidance

1. www.bt.cdc.gov CDC: links to CDC bioterrorism resources, reports of field investigations, and fact sheets.
2. www.cbaci.org/CDCSectionLinksMain.htm Chemical and Biological Arms Control Institute: extensive report and manual on the public health danger and response to bioterrorism.
3. www.emergency.com/cbwlesn1.htm Emergency Response and Research Institute: specific guidance on how to manage an incident.
4. www.vnh.org/FM8284/index.html U.S. Armed Forces, Virtual Naval Hospital: electronic manual provides specific guidance on the diagnosis, treatment, and management of biological warfare casualties.

5. www.usamriid.army.mil/education/bluebook.html U.S. Army Medical Research Institute of Infectious Diseases: provides electronic access to a manual describing specific measures for managing bioterrorism casualties.
6. <http://chemdef.apgea.army.mil/textbook/contents.asp> Electronic copy of the textbook Medical Aspects of Chemical and Biological Warfare, published by the U.S. Army Medical Research Institute of Chemical Defense.

Link directories to websites and electronic resources

1. www.apha.org/united the American Public Health Association (APHA): links to APHA publications and other websites concerning bioterrorism.
 2. www.ama-assn.org The American Medical Association: The AMA home page contains a link to a bioterrorism web site with news, additional links, and resources.
 3. www.apic.org/bioterror Association for Practitioners of Infection Control: overview of bioterrorism and links to electronic resources.
 4. www.cbiac.apgea.army.mil Chemical and Biological Defense Information Analysis Center: contracted to the Department of Defense, this website provides extensive links.
 5. www.hhs.gov/hottopics/healing/biological.html Department of Health and Human Services: Biological Incidents Preparedness and Response: links to various web resources concerning bioterrorism.
 6. www.hopkins-biodefense.org Johns Hopkins University Center for Civilian Biodefense Studies: comprehensive resource on bioterrorism.
 7. www.mlanet.org/resources/caring/resources.html Medical Library Association: comprehensive list of bioterrorism websites and print references.
 8. <http://bioterrorism.slu.edu> St. Louis University Center for the Study of Bioterrorism and Emerging Infections website and link directory.
 9. www.hshsl.umaryland.edu/resources/terrorism.html University of Maryland Health Sciences Library directory to electronic resources on bioterrorism.
 10. www1.umn.edu/cidrap University of Minnesota, Academic Health Center, Center for Infectious Disease and Research Policy website with news and educational links.
 11. www.usamriid.army.mil/links/bdr.htm USARMID: extensive link directory to bioterrorism websites and resources.
 12. www.fda.gov/oc/opacom/hottopics/bioterrorism.html U.S. Food and Drug Administration Bioterrorism Page: provides links to primarily Federal web sites and electronic documents concerning bioterrorism.
 13. www.foodsafety.gov/~fsg/bioterr.html U.S. Food and Drug Administration in conjunction with other government agencies web page on food safety, provides links to various websites focused on food safety and bioterrorism.
-

News, public policy, and opinion

1. www.biohazardnews.net Private website and free electronic newsletter with news, information, links, and opinion.
2. www.fas.org/bwc/index.html Federation of American Scientists Chemical and Biological Arms Control Program: news, public policy, links to electronic documents.
3. www.newscientist.com/hottopics/bioterrorism New Scientist: electronic news and commentary on bioterrorism.
4. www.stimson.org The Stimson Centre: news and views on chemical and biological weapons.

REFERENCES

1. JB Tucker. Historical trends related to bioterrorism: An empirical analysis. *Emerging Infectious Diseases*. 5[4]: 498-504, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
2. LD Rotz, AS Khan, SR Lillibridge, SM Ostroff, JM Hughes. Public health assessment of potential biological terrorism agents. *Emerging Infectious Diseases*. 8[2], 2002. In press. (www.cdc.gov/ncidod/EID/vol8no2/01-0164.htm).
3. Associated-Press. Report: Army lab was missing samples. *The New York Times* 2002 January 22, 2002. nytimes.com.
4. J Stern. The prospect of domestic bioterrorism. *Clinical Microbiology Reviews*. 5[4]:517-522, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
5. L Henry. SUN Profile: Harris' troubled past includes mail fraud, white supremacy. *Las Vegas Sun* 1998. (www.lasvegassun.com/dossier/crime/bio/harris.html).
6. CDC. Bioterrorism alleging use of anthrax and interim guidelines for management -- United States, 1998. *Morbidity and Mortality Weekly Report*. 48(04):69-74, 1999.
7. CDC. Update: Investigation of bioterrorism-related anthrax and interim guidelines for clinical evaluation of persons with possible anthrax. *Morbidity and Mortality Weekly Report*. 50[43]:941-948, 2001.
8. GW Christopher, TJ Cieslak, JA Pavlin, EM Eitzen. Biological warfare: A historical perspective. *Journal of the American Medical Association*. 278[5]:412-417, 1997.
9. WF Kleitmann, KL Ruoff. Bioterrorism: Implications for the clinical microbiologist. *Clinical Microbiology Reviews*. 14:364--381, 2001.
10. JEM Eitzen, ET Takafuji. Historical overview of biological warfare. In: Sidell FR, Takafuji ET, Franz DR, Eds. Medical Aspects of Chemical and Biological Warfare.

Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center;. 415-424, 1997.

11. MG Kortepeter, GW Parker. Potential biological weapons threats. *Emerging Infectious Diseases*. 5[4]:523-527, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
12. TW McGovern, AM Friedlander. Plague. In: Sidell FR, Takafuji ET, Franz DR, eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 479-502, 1997.
13. CJ Davis. Nuclear blindness: An overview of the biological weapons programs of the former Soviet Union and Iraq. *Emerging Infectious Diseases*. 5[4]:509-512, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
14. KB Olson. Aum Shinrikyo: Once and future threat? *Emerging Infectious Diseases*. 5[4]:513-516, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
15. DR Franz, CD Parrott, ET Takafuji. The U.S. biological warfare and biological defense programs. In: Sidell FR, Takafuji ET, Franz DR, Eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 425-436, 1997.
16. G O'Neal. Behind the biowarfare 'Eight Ball.'. *USA Today* 2001 December 20, 2001. 10D.
17. K Alibek. *The Chilling True Story of the Largest Covert Biological Weapons Program, Told from the Inside by the Man Who Ran It*. N.Y.: Random House, Inc.; 1999.
18. DA Henderson. Bioterrorism as a public health threat. *Emerging Infectious Diseases*. 4[3]:488-492, 1999. (www.cdc.gov/ncidod/eid/vol5no4/contents.htm).
19. AM Friedlander. Anthrax. In: Sidell FR, Takafuji ET, Franz DR, eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 467-478, 1997.
20. MN Swartz. Recognition and management of anthrax - An update. *New England Journal of Medicine*. 345[22]:1621-1626, 2001.
21. TV Inglesby, DA Henderson, JG Bartlett, al. e. Anthrax as a biological weapon: Medical and public health management. *Journal of the American Medical Association*. 281[18]:1735-1745, 1999.
22. A Salyers, D Whitt. Bioterrorism (Rapid Response Chapter). . *Microbiology: Diversity, Disease, and the Environment*. Bethesda, MD: Fitzgerald Science Press, Inc. 2001. www.fitzscipress.com.

23. M Meselson, J Guillemin, M Hugh-Jones M, et al. The Sverdlovsk anthrax outbreak of 1979. *Science*. 266:1202-1208, 1994.
24. Anonymous. Drugs and vaccines against biological weapons. *The Medical Letter*. 43[115]:87-89, 2001.
25. PK Russell. Vaccines in civilian defense against bioterrorism. *Emerging Infectious Diseases*. 5[4]:531-533, 1999.
26. L Liedtke. HHS statement on anthrax vaccination. Vol. 2001: Infectious diseases Society of America and the Centers for disease Control and Prevention. 2001.
27. CDC. Update: Investigation of bioterrorism-related anthrax Connecticut, 2001. *Morbidity and Mortality Weekly Report*. 50[48]:1077-1079, 2001.
28. ND Kristof. Profile of a killer. *The New York Times* 2002 January 4, 2002. A21.
29. DJ McClain. Smallpox. In: Sidell FR, Takafuji ET, Franz DR, eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 539-559, 1997.
30. DA Henderson, TV Inglesby, JG Bartlett, al. e. Smallpox as a biological weapon: Medical and public health management. *Journal of the American Medical Association*. 281[22]:2127-2137, 1999.
31. E Susman. ICAAC: Stored smallpox vaccine still potent enough to protect individuals, even at 10-to-1 dilution. *Doctors Guide to the Internet* @ <http://docguide.com> 2001 December 19, 2001.
32. LA Coyle. The nation; When smallpox failed. The New York Times 2001 December 2, 2001. Late Edition - Final, Section 4, Page 5, Column 1.
33. S Brownlee. Clear and present danger. *The Washington Post* 2001 October 28, 2001. W08.
34. ME Evans, AM Friedlander. Tularemia. In: Sidell FR, Takafuji ET, Franz DR, Eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 503-512, 1997.
35. DT Dennis, TV Inglesby, DA Henderson, al. e. Tularemia as a biological weapon: Medical and public health management. *Journal of the American Medical Association*. 285[21]:2763-2773, 2001.
36. TV Inglesby, DT Dennis, DA Henderson, al. e. Plague as a biological weapon: Medical and public health management. *Journal of the American Medical Association*. 283[17]:2281-2289, 2000.

37. PB Jahrling. Viral hemorrhagic fevers. In: Sidell FR, Takafuji ET, Franz DR, eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 591-602, 1997.
38. CDC. Management of patients with suspected viral hemorrhagic fever. Morbidity and Mortality Weekly Report. 37 [S-3]:1-16, 1988.
39. DN Gilbert, RC Moellering, MA Sande. The Sanford Guide to Antimicrobial Therapy 2001. 31st edition, Hyde Park, Vermont: Antimicrobial Therapy, Inc. 2001.
40. JL Middelbrook, DR Franz. Botulinum toxins. In: Sidell FR, Takafuji ET, Franz DR, Eds. Medical Aspects of Chemical and Biological Warfare. Washington, D.C.: Office of the Surgeon General at TMM Publications, Borden Institute, Walter Reed Army Medical Center. 643-654, 1997.
41. SS Arnon, R Schechter, TV Inglesby, al. e. Botulinum toxin as a biological weapon. *Journal of the American Medical Association*. 285[8]:1059-1070, 2001.

6

Weaponization and Delivery Systems

Mark A. Prelas

University of Missouri, Columbia, Missouri

The specter of biological weapons has haunted mankind for nearly a thousand years. Until recently, biological weapons have been viewed as strategic weapons. As a strategic military tool, biological weapons are very limited. They are highly dependent upon the weather, temperature, wind direction, wind speed and other factors that cannot be controlled. However, with the proliferation of information that an open society offers, the know-how to develop and use biological weapons is becoming available to individuals. Thus, biological weapons must now be viewed as a much broader threat. Biological weapons have a psychological effect upon people as they can create terror among the masses. This makes biological weapons an ideal tool for terrorism.

We review here the weaponization of biological agents and the delivery systems that were designed for efficient dispersal of the agents both for military and domestic terrorist attack.

HISTORY OF BIOLOGICAL WEAPONS

We begin our examination of the uses of biological weapons in the pre-World War II era.

- The use of biological agents is believed to have happened much earlier than that recorded in the history. One of the first uses of biological agents occurred in 1346 during the siege of the Genoese city of Caffa (located in present day Feodosia, Ukraine). The Tartars, believing that the Europeans were responsible for an epidemic of the plague in Asia, initiated a siege against the Genoese-controlled city. The cadavers of plague victims were

catapulted to Genoese City [1]. One of the significant dangers of using biological weapons manifested itself in the siege of Caffa. A few Genoese merchants escaped Caffa by sailing home and took the illness with them. Ships with infected rats arrived from Caffa at the port of Messina, Sicily in 1347 and the disease spread from there. Europe was plunged into an epidemic and after five years 25 million people or about one-third of Europe's people were killed. The impact of the plague was probably magnified by the superstitions of Europeans who believed that cats, the natural predator of rats, were witches. Cats were killed because of this superstition. This epidemic was referred to as the "black death."

- In 1710 during the war between Russia and Sweden, Russia adopted the Tartar tactic from the siege of Caffa and used the bodies of plague victims to expose Swedish soldiers.
- Perhaps the most effective use of a biological agent in warfare occurred during the French and Indian War of 1776. Sir Jeffery Amherst ordered the use of blankets and handkerchiefs that had been used in a smallpox hospital to be delivered to the Indians loyal to France [2]. An officer who delivered the infected cloth wrote in his journal "I hope it will have the desired effect." Indeed it may have had its desired effect. Sir Jeffery Amherst was able to take Fort Carlillon due to the weakened state of the Indians and he renamed it Fort Ticonderoga.
- In 1917, during World War I, German agents infected allied horses and cattle with glanders before they were shipped to the European front.

The means of finding effective biological agents and delivering those agents to the enemy is a complex problem. Not until the application of 20th century science did biological agents become a legitimate military threat. The era from World War II to the present represents the application of 20th century science to the weaponization of biological agents. As is known from aerosol science (see Chapter 4) particles with a mean distribution of below 5 micrometers are the most effective way of infecting a human (host) with a biological agent. The weaponization of a biological organism requires:

- Good agent properties: virulence, stability to heat, stability in air, stability in humidity, stability to ultraviolet light, can be concentrated, can be dried, can be made into 1 to 5 micrometer particles and can survive in aerosol form.
- The munitions: biological agents have to be delivered to the target efficiently.

- Meteorological conditions: atmospheric conditions such as wind speed, wind direction and humidity need to be optimum. If the wind blows in the wrong direction, the agent will not disperse over the target. If it is raining, then the aerosol washes out of the air.

- Method of dissemination: spray (line source) or explosion (point source).

- If the agent is sensitive, an explosion might destroy it. The start of the modern era of the biological weapons began with the Japanese biological weapon program with the formation of Unit 731 between 1937-45. Unit 731 performed experiments on Chinese, Russian and American prisoners to determine which diseases could best serve as weapons. The program successfully used a biological weapon in 1940. Japan dropped plague-infected fleas on areas in China and Manchuria and caused the outbreak of plague [1, 3].

The U.S. program began in 1941 when intelligence indicated that Germany and Japan were involved in biological weapons research. Secretary of War, Henry L. Stimson, requested the National Academy of Science to review the feasibility of manufacturing biological weapons. In 1942 a committee formed the National Academy of Science concluded that biological weapons were feasible. As a result George W. Merk was asked by the Secretary of War to form the War Reserve Service. Camp Detrick in Frederick, Maryland, was chosen as the War Reserve Service's primary site. The site became operational in 1943. In 1944, Dugway proving grounds in Utah was established as a test center for the program. Additionally, a production plant was built in Terre Haute, Indiana. During 1947-49 small-scale tests of simulated biological agents, *Bacillus Globigii* (BG) and *Serratia Marcescens* (SM), were performed at Camp Detrick. *Serratia Marcescens* is a harmless bacterium that is easily tracked due to its bright red color. For example, instructors in medical school used it to demonstrate the transmission mechanisms for infectious diseases. An instructor would put the organism in his or her mouth and then lecture. The organism would be captured on plates covered with nutrients around the room. The next day, the dispersion of SM around the room could be seen on the plates by its characteristic color. *Bacillus Globigii* is used as a simulant for anthrax because it too forms a spore like anthrax, but harmless to humans.

In 1950, the U.S. biological weapons program was extended due to the Korean War. An anti-crop bomb was developed by 1951 and was placed into production. The U.S. program had looked at 2000 potential plant pathogens. Of those, 551 could be potential threats to our agricultural industry. These include rice blast, late blight of potato, stem rust of wheat, stem rust of rye, southern corn leaf blight, and citrus canker.

In 1953, the Camp Detrick program was expanded and the construction of large-scale production of biological agents was underway. A large-scale production facility was established in Pine Bluff, Arkansas, and it became operational in the same year. By 1954 tularemia was being produced at the Pine Bluff plant.

Soviet Minister Marshal Zhukov, added fuel to the fire in 1955 when he stated that the USSR would use chemical and biological weapons in future wars.

From 1959-69 the military services submitted requirements for biological weapon munitions including artillery shells, missiles, drones and other weapons. With emphasis on munitions, the Desert Test Center (DTC) was established at Ft. Douglas, Salt Lake City in 1962. In 1964-66 the virus and rickettsiae production plants were built at Pine Bluff, Arkansas.

The U.S. also engaged in simulations using harmless bacterium to demonstrate the potential of biological weapons [3, 4]. In 1949, attack teams with sprayers introduced SM into the intake vents of the Pentagon's air conditioning system. Had this been a real anthrax attack, half of the military's top command would have been killed. This simulated attack convinced the military that biological weapons were a threat.

In order to demonstrate the threat to the U.S. population, in April of 1950 the USS Coral Sea and USS K. D. Bailey sprayed both SM and BG into the wind blowing towards Norfolk, Hampton, and Newport News, Virginia. The tests demonstrated that U.S. coastal cities could be threatened by a biological attack.

In September 1950, about two miles off the coast of San Francisco, U.S. Navy ships sprayed SM, BG and a cloud of fluorescent particles, along a dissemination line of 3 miles length. The material was collected at monitoring stations around the bay area. The Fluorescent Particles (FP) deposited throughout the city's streets and sidewalks and at night, under ultraviolet light glowed like stars. Traces of SM, BG and FP were found as far away as twenty-three miles. If the organism had been anthrax, it would have produced lethal doses in an area of about 50 square miles.

A series of tests were designed to show that a large-scale attack with biological weapons was feasible. On December 2, 1957, an AC-119 sprayed an area from South Dakota to International Falls, Minnesota, with fluorescent particles while a cold air front was moving down from Canada. Particles were detected 1200 miles away in New York State.

A plane flying from Toledo, Ohio, to Abilene, Texas, and a second plane flying from Detroit, Michigan, to Goodland, Kansas, sprayed about forty pounds of FP per minute. Sampling stations on the ground proved that large areas of the country could be attacked with biological weapons.

A jet aircraft equipped with a BG sprayer flew a predetermined pattern near Victoria, Texas. The BG was found as far East as the Florida Keys.

Travelers at the Greyhound Bus terminal in Washington D.C., and the Washington National Airport, Washington D. C., were subjected to BG in October 1965. Scientists walked through the bus terminal and the airport and sprayed the bacterium into the air without being detected. Aerosol traps were placed at strategic points to capture the bacterium as it moved through the air.

A light bulb filled with BG was dropped on the tracks in the New York City subway in June 1966. BG spread throughout the subway system within 20 minutes. Monitoring of the BG demonstrated that even this small amount of material, had it been anthrax, could have killed thousands of people.

Overall, more than 200 tests were performed to demonstrate the potential of biological weapons. This research culminated between 1964 and 1968 with a series of tests at facilities in the Pacific including the well-known project SHADY GROVE. The tests demonstrated that a single weapon was able to cover 2400 square kilometers with 30% casualties [3].

President Nixon of the U.S.A. renounced the use of biological weapons in 1969. This marked the beginning of the end of the U.S. biological weapons program. Between 1970-72 all biological weapon stocks were destroyed and in 1975 President Ford signed the Biological Weapons Convention along with 144 countries.

The biological weapons program in the USSR has been shrouded in secrecy since its inception in the 1920s. The first weapons used were low flying airplanes with crop sprayers. After World War II, bombers armed with an explosive dispersion system were added. However, until the defection of Vladimir Pasechnik in 1989 and Ken Alibek (formerly Kanaftjan Alibekov) in 1992 the full extent of the USSR program was not known [5]. After signing the Biological Weapons Convention in 1972, the USSR developed an extensive program for the production of biological agents in sufficient quantities to load multiple-warhead ballistic missiles and cruise missiles. An extensive network of production facilities were built for the Ministry of Defense under the direction of the Fifteenth Directorate, the Ministry of Medical and Microbiological Industries under the direction of Biopreparat, the Ministry of Health under the Second and Third Main Directorate and the Ministry of Agriculture under the direction of the Main Directorate for Industrial Production and Scientific Enterprise [5]. Techniques were developed for the weaponization of anthrax (antibiotic resistant), brucella, smallpox, tularemia, Q-fever, glanders, plague, Marburg variant U, Lassa fever, monkey pox and Ebola. By 1987 the USSR could produce 5000 tons of anthrax per year or 80 to 100 tons of smallpox per year [5]. Of most concern was the USSR's program to genetically engineer new agents [5].

The Russian Government has opened many of the Biopreparat sites to the international community. Dr. Alebek has expressed his concern however, that many of the sites of the Fifteenth Directorate are still not open to the west for inspection.

MUNITIONS

The weaponization of biological agents requires that they be dispersed by the most effective means possible. Military weapons dispense and disperse their submunitions payload from a primary unit in order to maximize the spread of the biological agent by the delivery system. The primary unit is the shell, missile or cruise missile that carries the submunitions (Figure 6.1).

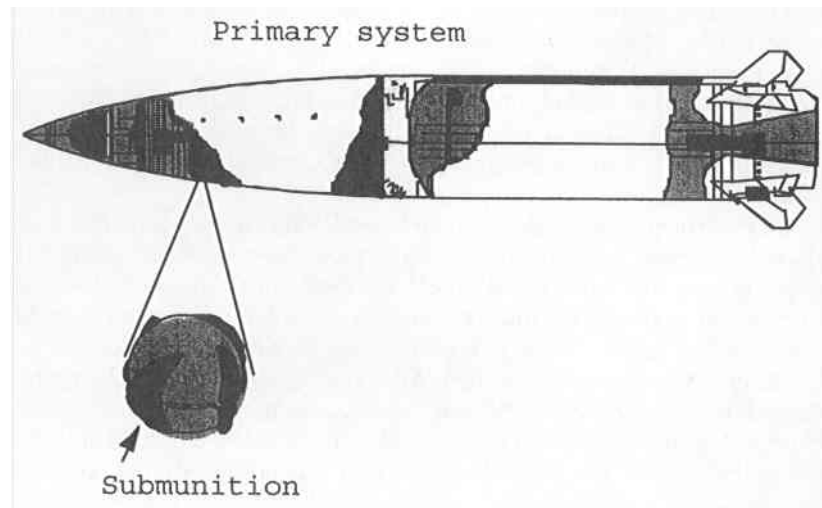


Figure 6.1 Primary system loaded with submunitions [6].

Dissemination of biological agents may be achieved by releasing or discharging the agents from munitions or submunitions by pressurized gas or an explosive to form an aerosol. The stability of the agent determines if the agent can be released by explosives or by pressurized gas. The submunitions can be of the spherical design, as shown in Figure 6.1 or a Flettner rotor design for wider dispersal patterns. Less sophisticated designs such as a dart or cylinder can be used for a more compact dispersal pattern.

The system does not have to be complex to be of concern. Iraq purchased the widely available R-400 bomb for biological agent dispersal [7]. A diagram of how the R-400 can be adopted for biological agent dispersal is shown in Figure 6.2.

It is possible to use sprayers mounted on cruise missiles to disperse biological agents. This method produces a line source and is a very efficient means of disseminating biological agents (See Figure 6.3). Due to the proliferation of cruise missiles, this possibility is very real [8].

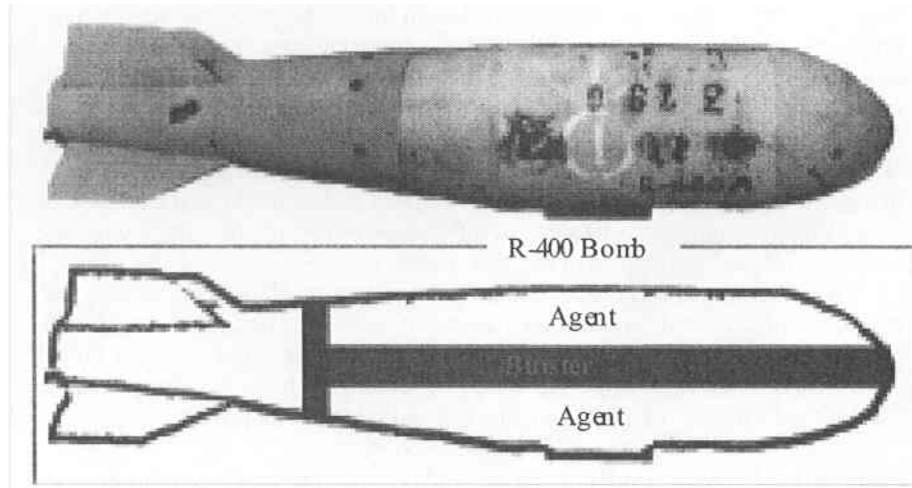


Figure 6.2 Use of an R-400 bomb for biological agent dispersal.

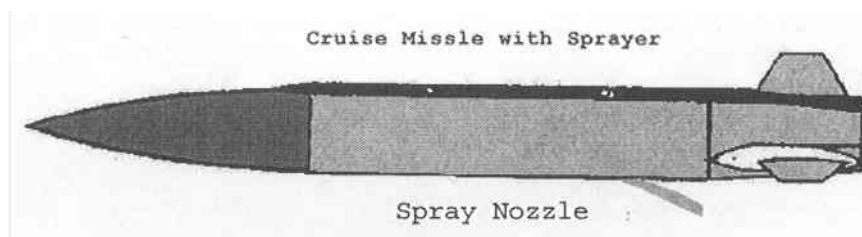


Figure 6.3 A cruise missile equipped with a sprayer (similar to the Russian made TMU-28/B).

Biological agents can be ingested in the gastrointestinal system, they can be introduced into the lungs by aerosols, or the skin may absorb the agent. In modern biological weapons, the dispersal method of choice is by aerosol. Specifically, particles with 1 to 5 micrometer diameter are called the primary aerosol. The primary aerosol flows rather easily and a person becomes infected because he or she is breathing at a rate of 10 to 20 liters of air per minute. Each aerosol particle will contain a number of infectious organisms. The goal of dissemination of biological agents is to put as many infectious organisms in the vulnerable areas of the human body as possible. Aerosol particles having diameter in the range of 18 to 20 micrometer deposit in the sinus. The sinus is the least infectious area of the pulmonary system. Particles of 15 to 18 micrometer in diameter can deposit in the throat. The throat is a slightly more infectious area than the sinus. Particles in the

7 to 12 micrometer in diameter will deposit in the esophagus. This area is more infectious than the throat but is not the most sensitive region. The most infectious area is in the lungs where particles of 4 to 6 micrometers deposit in the bronchioles and particles of 1 to 3 micrometer deposit in the alveoli. Alveoli are the most vulnerable areas within the lungs. Therefore, an ideal biological weapon would be the one that would disperse biological aerosols in the size range of 1 to 3 micrometer in diameter. Table 6.1 shows the infective dose of various biological agents. This table also points out whether or not an infected person would transmit the disease to another person by coughing or by other mechanisms.

The number of organisms required to cause an infection is the next important factor because it determines the number of aerosol particles that must be deposited. In Table 6.1, the number of organisms required to infect a human host is shown for several biological organisms. In addition, the table indicates if the organism can be passed from a person who is infected to another person.

Table 6.1 Infective dose of an organism and potential transmission from one person to another [9].

Disease	Transmits Human to Human	Infective Dose (Aerosol)
Inhalation anthrax	No	8,000-50,000 spores
Brucellosis	No	10 -100 organisms
Cholera	Rare	10-500 organisms
Glanders	Low	Assumed low
Pneumonic Plague	High	100-500 organisms
Tularemia	No	10-50 organisms
Q Fever	Rare	1-10 organisms
Smallpox	High	Assumed low (10-100 organisms)
Venezuelan Equine Encephalitis	Low	10-100 organisms
Viral Hemorrhagic Fevers	Moderate	1-10 organisms
Botulism	No	0.001 $\mu\text{g}/\text{kg}$ is LD_{50} for type A
Staph Enterotoxin B	No	0.03 $\mu\text{g}/\text{person}$ incapacitation
Ricin	No	3-5 $\mu\text{g}/\text{kg}$ is LD_{50} in mice
T-2 Mycotoxins	No	Moderate

Table 6.2 The amount of biological agent required to produce a LD₅₀ in a one square kilometer area.

Agent	Kilograms of agent required to produce a LD ₅₀ over one square kilometer
Anthrax	0.007
Plague	0.00009
SEB	40
Botulinum	60
Ricin	600

With the infective dose, and assumptions about the number of microorganisms per aerosol particle, one can calculate the amount of aerosol that is required to infect a building of one square kilometer in area (See Appendix 6.1).

We introduce here the concept of the LD₅₀—the lethal dose (LD) that will kill 50% of the exposed population. Biological agents are the most effective weapons (as compared to chemical and nuclear weapons) in terms of the amount of material needed for lethality (See Table 6.2).

Biological weapons can impact a larger area than nuclear or chemical weapons (See Table 6.3). Biological weapons are less expensive than nuclear or chemical weapons.

Table 6.3 Relative comparisons of destruction power of nuclear, chemical and biological weapons.

Parameter	Nuclear	Chemical	Biological
Affected area (square miles)	~100	~100	~2,000
Human Lethality	98%	30%	Up to 75% depending on agent
Residual Effect	6 months of radioactive fallout on ~1000 sq miles	3-36 hours over the same area	Potential epidemic depending on agent
Time for effect	Millisecond	Seconds	Days
Property damage	~40 sq. miles	None	None

It is important to note that Table 6.3 assumes ideal weather conditions for dispersion of chemical and biological agents.

SMALL-SCALE DEPLOYMENT

Biological weapons can be successfully deployed on a small-scale. For example, in September of 2001, weapons grade anthrax was sent through the mail in envelopes to various broadcasting news channels [10]. The letters also went to U.S. Senators Tom Daschle and Patrick J. Leahy. At the time of this writing, the source of the anthrax was unknown, however it was of a weapon grade comparable to material developed by the U.S. earlier [11, 12]. The particles making up the powder did not have an electrostatic charge and thus did not agglomerate. Material of this quality can be disseminated by a variety of methods. These may include spraying (from a dry powder garden sprayer to a crop duster), airborne release from a container (such as breaking a glass jar), to just throwing it into the air.

A highly infectious agent such as smallpox could be a devastating weapon even on a small-scale. Due to the eradication of smallpox in 1972, the natural resistance to the smallpox virus in the human population should be fairly weak. Additionally, smallpox vaccinations given prior to 1972 are probably no longer effective. Officially, there should be only two seed samples of live smallpox virus left in the world, one in the U.S. and another one in Russia. However, one cannot discount the existence of other samples. If a terrorist were to be exposed to smallpox, it would be feasible for that terrorist to infect a planeload of people on a long haul flight while in the infectious stages of the disease. Given the nature of travel across borders today as compared to 1972, it would be very difficult to implement quarantine along with vaccination as a means of containment. There is a potential of spreading smallpox worldwide.

CONCLUSIONS

The biological weapons programs of the United States and the former USSR committed substantial resources to the understanding of the science and technology. Biological agents were weaponized. Information from these programs is filtering out into the public domain and is the cause of great concern for the proliferation of biological weapons. There is little doubt that the technology has proliferated to countries. Even groups, cults and individuals are beginning to acquire the knowledge. There are recent examples. The Aum Shinrikyo had tried to deploy anthrax in Japan several times from 1993-1995 but failed [5]. In addition, at the time of this writing, The Times of London reported that it had discovered documentation in Afghanistan that al-Qaeda had a keen interest in developing biological weapons [13].

APPENDIX 6.1 CALCULATION OF MASS OF ANTHRAX MATERIAL REQUIRED TO PRODUCE A LD₅₀ IN A VOLUME V

Consider M (kg) of anthrax-infected aerosol is dispersed in a volume of V (m³) of air. The mass concentration assuming no settling and other losses is given by:

$$M/V \text{ (kg/m}^3\text{)} \quad \text{Eq. 6.1}$$

Assuming an average particle diameter of d, the number concentration is:

$$N = (M/V)/(\pi d^3 \rho/6) \text{ (number of particles/m}^3\text{ of air)} \quad \text{Eq. 6.2}$$

where, ρ is average density of the particles in kg/m³. If each aerosol particle contains J anthrax spores then the number of spores per cubic meter of air is:

$$N_s = N J \text{ (spores/m}^3\text{)} \quad \text{Eq. 6.3}$$

If the volume of air that an average person breaths per minute is V_b (m³/minute), the rate of spores that a person breaths in per minute is:

$$R_s = N_s V_b \text{ (spores/min)} \quad \text{Eq. 6.4}$$

A Lethal Dose-50 (LD₅₀) is the number of organisms that would cause the death of 50% of the people receiving that dose. To receive a LD₅₀, an average person would need to accumulate a total of A (spores/LD₅₀) anthrax spores. Thus the multiples of LD₅₀ (X) accumulated over an exposure time T (minutes) is:

$$X = A/TR_s \quad \text{Eq. 6.5}$$

Assuming that you want X to be a single multiple of LD₅₀ per exposure time, one can set Equation 6.5 equal to one and then derive Equation 6.6 using Equations 6.3 and 6.2-a formula for the required mass of aerosol to infect a given volume of space with one LD₅₀ over an exposure time T.

$$M = A(V/TV_b)(\pi d^3 \rho/6)/J \text{ (kg)} \quad \text{Eq. 6.6}$$

REFERENCES

1. L Pringle. *Chemical and Biological Warfare: The Cruellest Weapons*. Hillside: Enslow Publishers, Inc., 1993.
2. GW Christopher, TJ Cieslak, JA Pavlin, EM Eitzen, Jr. Biological warfare: A historical perspective. *Journal of the American Medical Association* 6: 412-418, Aug 1997.
3. E Regis. *The Biology of Doom*. New York: Henry Holt and Company, 1999.
4. FAS (Federation of American Scientists). *Biological Weapons*. <http://www.fas.org/nuke/guide/usa/cbw/bw.htm>
5. K Alibek. *Biohazard*. New York: Random House, 1999.
6. US Army 2. *The Army Tactical Missile System. Special Text 6-60-30*. www.army.mil/gunnery/manuals/afom/afom.doc, 2000.
7. RD Walpole. Intelligence related to possible sources of biological agent exposure during the Persian Gulf war. <http://www.gulfink.osd.mil/library/43917.htm>, 2000.
8. Centre for Defence and International Security Studies (CDISS). <http://www.cdiss.org/cruise1.htm>, 2000.
9. US Army 1. *Medical Research Institute of Infectious Disease*. <http://www.biomedtraining.org/materials.htm>, 2000.
10. E Lipton, J Kirk. Months later, scientists know where anthrax outbreak began. *St. Louis Post Dispatch*. December 26, 2001. (<http://home.post-dispatch.com/channel/pdweb.nsf/TodayWednesday/86256A0E0068FE5086256B2E003C2973?OpenDocument&PubWrapper=A-section>).
11. WJ Broad. Terror anthrax linked to type made by U.S. *New York Times*, December 3, 2001. (<http://www.nytimes.com/2001/12/03/national/03POWD.html>).
12. WJ Broad, J Miller. A nation challenged: The investigation; U.S. recently produced anthrax in a highly lethal powder form. *New York Times*, 12/13/01. (<http://query.nytimes.com/search/abstract?res=F20F16FF385B0C708DDDAB0994D9404482>).
13. A Loyd. Scientists confirm Bin Laden weapons tests. *The Times*, London, December 29, 2001.

BIBLIOGRAPHY

- W Allen. Army tests conducted here in the 1950s showed how biological agent might spread. Zinc cadmium sulfide particles were sprayed from street corners in a city. St. Louis Post-Dispatch (MO), page A10, September 20, 2001.
- General Accounting Office. Biological Weapons, GAO/NSIAD-00-138, Effort to reduce former soviet threat offers benefits, poses new risks. April 2000.
- General Accounting Office. Bioterrorism, GAO-01-915 Federal Research and Preparedness Activities. September 2001.
- SM Hersh. Chemical and Biological Warfare. Garden City: Doubleday and Company, Inc., 1969.
- B Lambrecht. Planning for bioterrorism attack takes on a new urgency for U.S. government prepares for worst-case scenario with drills, training. St. Louis Post Dispatch (MO), page A10, September 20, 2001.

7

The Classification and Manufacture of Biological Agents

Mark A. Prelas

University of Missouri, Columbia, Missouri

Biological agents are living organisms or the toxins generated by living organisms that cause disease in humans, animals, or plants. These agents can be bacteria, virus, mycoplasma or toxin as described in Chapter 5. The agent may be lethal or incapacitating.

Biological agents can be produced by four methods. The most common means of producing bacterial agents is by fermentation. Viral agents are most commonly produced by the inoculation of fertile eggs. Both viral and bacterial agents can be produced in live animals or in tissue. Toxins are derived as a byproduct of the growth of a biological organism just as alcohol is a byproduct of the growth of yeast. Toxins can also be derived from snakes, insects, spiders, sea creatures and plants

CLASSIFICATION OF AGENTS

Biological agents can be used as antipersonnel agents that are effective against humans. They may also be employed as antianimal, antiplant and antimaterial agents. Antianimal agents are effective against animals. Antiplant agents are live organisms that cause disease or damage to plants. Antimaterial agents cause damage or breakdown of materials such as rubber.

Potential bacterial agents that may be used in a biological warfare include anthrax (*Bacillus anthracis*), plague (*Yersinia pestis*), tularemia (*Francisella tularensis*), salmonella (*Salmonella typhi*), and cholera (*Vibrio cholerae*). There are a host of other bacterial and antimaterial agents that can be used for domestic terrorist attack. There are many other potential bacterial agents as discussed in US Army,

Medical Research Institute of infectious disease, Biological Casualties Handbook, 2000.

Agents can also be derived from the family of organisms called rickettsiae such as Q-fever (*coxiella burnetti*).

Viral agents are composed of DNA (e.g., smallpox) or RNA (viral hemorrhagic fevers such as Ebola, Marburg and Congo-Crimean) that requires living cells to replicate. Examples of other viral agents are Dengue fever, encephalitis (e.g., Venezuelan equine, West Nile, Japanese, Western equine and eastern equine), monkey pox, white pox, Rift Valley fever, Hantaan virus and yellow fever.

Toxins are poisonous chemicals that are produced by the metabolic activities of living organisms. These agents are organic chemical compounds such as proteins, polypeptides and alkaloids. Toxins can be categorized in two ways: neurotoxins that affect nerve impulse transmission and cytotoxins that destroy or disrupt cells. Toxins can be derived from bacteria and they can be either exotoxins (poisons that diffuse out of cells) or endotoxins (poisons contained in the cell but are released when the cell disintegrates). Toxins produced by fungi are called mycotoxins. Mycotoxins are exotoxins that include tichothecenes (which may be the source of yellow rain discussed in Chapter 6), aflatoxins (produced by *aspergillus flavus*) and temorgens (which affect the nervous system). Toxins can be produced from plants such as castor beans (ricin) and abrus seeds (abrin) and algae (anatoxin A from blue-green algae). Finally, a number of toxins are generated by animals such as batrachotoxin from a frog, palytoxin from soft corals, saxitoxin from shellfish, comotoxins from sea snails, tetrodotoxin from puffer fish, snake venom and spider venom.

THE FUTURE OF BIOWARFARE IN THE BIOTECHNOLOGY AGE

Just as the atomic age began in the twilight of the industrial age, we are on the threshold of the biotechnology revolution. The human genome is well in hand and we are beginning to understand the aging process. Dreamers of this age foresee a time when replacement organs can be grown, viruses can be designed to attack diseases such as cancer, and the aging process is slowed down if not stopped. However, nature always seems to have a balance in that the promise of a technology is countered by its terror.

In his book, *Biohazard*, Dr. Ken Alibek relates a conversation with fellow Soviet Bioweaponer Dr. Lev Sandakchiev. According to Dr. Sandakchiev, it is possible to produce a "chimera virus". Chimera is a mythological beast with the head of a lion, the body of a goat and the tail of a serpent. To a bioweaponer, it is a virus that takes the property of lethality from one organism and mixes this with the infectious property of another. According to Dr. Alibek, one of the goals of the Soviet bioweapons program was to produce a smallpox-ebola weapon. These pioneers in the biotechnology age made substantial progress using crude tools such as

the search for promising mutations in nature when a new epidemic arises or mutations created in the growth of a large batch of agent in a Soviet bioweapon factory or perhaps the splicing of genetic material from one agent to another. As the tools of the biotechnology age grow, so grows the potential good and the potential mischief. Motivated bioweaponers of the future will likely have the tools to create the "chimera virus". It may take the form of a designer virus that can attack the genetic patterns of a specific individual or a whole ethnic group. If history has taught us one thing it is that knowledge cannot be stopped, only slowed down. The threshold of the biotechnology age is upon us for good or for evil.

MANUFACTURING PROCESS

Fermentation

Fermentation is a method of providing nutrients to biological organisms for rapid growth. A simple example of fermentation is the brewing of beer or wine. Here the biological organism is yeast and the growth of yeast produces alcohol as the byproduct. Fermentation is widely used in the pharmaceutical industry as well for production of a number of drugs. The widespread use of this technology along with basic understanding of the processes involved makes production of biological warfare agents by fermentation rather easy. As a result it is difficult to isolate or identify a fermentation facility that is designed or used exclusively for production of biological agents. The home brewing of beer and wine is simple and prevalent and the presence of brewing facilities in a home would be beyond suspicion.

Fermentation can be used to produce lethal bacteria such as anthrax or toxins such as botulinum from the growth of the bacteria *Clostridium botulinum*. Two methods for fermentation can be used. The first is the batch process in which a single fill of nutrients is used and the organisms grow until the nutrients are gone. The second method is continuous fermentation where nutrients are added as organisms are taken out. We will focus on the batch fermentation process because it is easier to implement and lends itself well to anaerobic (absence of oxygen) fermentation that is required for anthrax and botulinum toxin.

The first step in the batch fermentation process is to acquire a culture of the organism. The nutrients need to be prepared prior to the addition of the organism. The content of the nutrient mixture is highly dependent upon the organism that one wants to grow. In the case of brewing beer, malt is added as the nutrient and hops and grains are added for flavor (see Figure 7.1).

Once the nutrient is ready, the biological organism is added as shown in Figure 7.2 and the container is kept at a certain temperature that encourages growth of the organism. Other environmental conditions may be varied as well.



Figure 7.1 The author on the left and colleague (Dr. Malcolm Harris) use malt as the nutrient for the fermentation process.

This basic batch fermentation process can be used for growth of biological agents in large-scale using a fermenter having greater than 500 liters capacity [1, 2]. In large-scale production, the first step is to acquire a seed stock of the organism that will be grown. This seed stock can be obtained from many sources. For example, the US has the American Type Culture Collection in Rockville, Maryland. Prior to an incident in April 1995 involving Larry Harris, a member of a white supremacist group in Ohio, it was feasible to order cultures of deadly organisms from the American Type Culture Collection for \$35 by simply using an order form with a University letterhead. Mr. Harris tried to order three vials of plague from the American Type Culture Collection catalog. Mr. Harris did not realize that it took at least 30 days for the American Type Culture Collection to fill an order. He became impatient after two weeks and began to make telephone calls to the American Type Culture Collection. These calls raised suspicions and a subsequent investigation revealed Mr. Harris' plot. As a result, the American Type Culture Collection has implemented strict standards in their ordering process. However, in his book *Biohazard*, Ken Alibek reported that Iraq had picked up strains of anthrax, tularemia and VEE once targeted by the US biological weapons program for weaponization from the American Type Culture Collection prior to

the changes in the ordering process [1]. There are at least 90 other culture collections around the world and most are not as secure as the American Type Culture Collection.

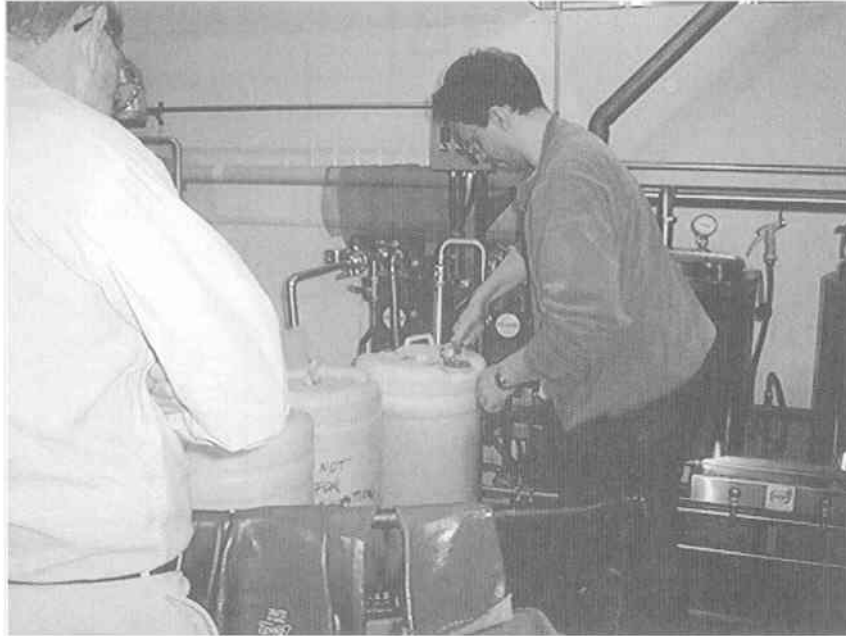


Figure 7.2 The biological organism (in this case yeast) is added to the nutrient. Environmental conditions such as temperature for optimum growth of the organism are then maintained.

Culture collectors obtain their samples of organisms from researchers and from outbreaks of disease in the human and animal populations around the world. The animal and human populations of the world are potential incubators for the growth of biological organisms. Mutations occur in large populations of the organisms and time or outbreaks facilitate the growth of large populations, thus it is important to collect samples from each outbreak to determine if the organism has mutated and to provide a stock of material for the production of a vaccine.

As shown in Figure 7.3, the second step is to put the seed organisms into a small container or flask filled with nutrients and to mix it thoroughly. The organisms start to grow with time. Afterwards, the contents of the flask are then put in a larger container or mid-sized fermentor and mixed. The organisms are then allowed to grow in the mid-sized fermentor. As the organisms approach their peak population, the contents of the mid-sized fermentor are transferred to a larger volume or large-size fermentor with additional nutrients. The organisms are allowed

to grow in the large-size fermentor until its population reaches a peak level. At this point in time, the contents of the large-size fermentor are placed in a centrifuge and the contents are separated and concentrated. In a weaponization process, additives are placed in the concentrated materials for performance purposes and the next step in the process is to dry the mixture. Once dried, the material is milled and sized. The resulting milled and sized material is then ready for use or storage. This technology exists. For example, the biological weapons program in the former Soviet Union demonstrated large-scale production of anthrax, smallpox, plague, and other agents [1, 2].

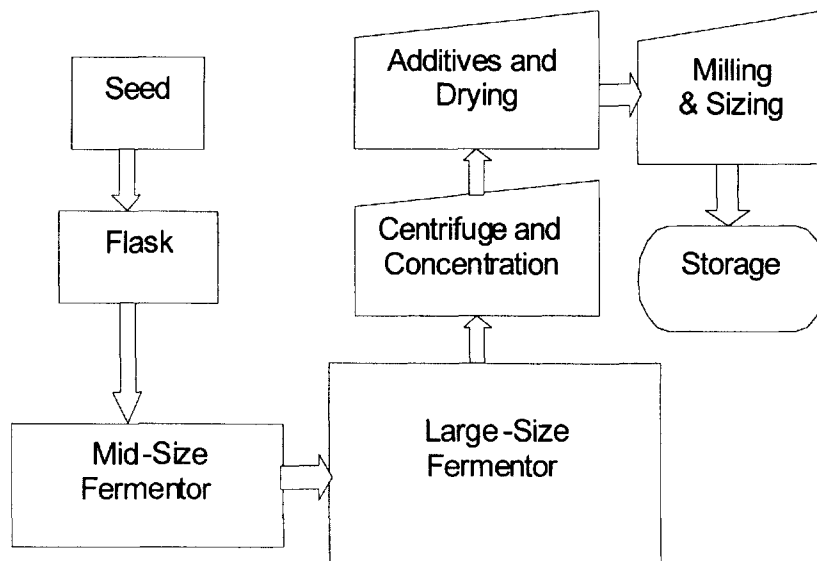


Figure 7.3 Diagram for large-scale fermentation of biological organisms.

Small Scale Fermentation

The batch fermentation process can be adapted to small-scale (typically less than 50 liters) production of biological organisms. For example, home brewing of beer or wine is very common and equipment necessary to set up a fermenter is easily available. As described above, the process of fermentation used for beneficial biological organisms is the same process that is used for the growth of lethal biological agents. For example, it is feasible to grow *clostridium botulinum* (the organism that produces botulism toxin) in a garbage can.

Viral Production Process

A viral agent requires the presence of cells in order to replicate. This requirement makes the viral agent more difficult to cultivate. Several methods are available and are discussed below.

One of the methods that is used for the production of viral agents is through the use of fertile chicken eggs. In this process, fertile chicken eggs are inoculated with the viral agent from seed stock. The egg is allowed to incubate until the viral organism population has peaked. The embryo from the egg is harvested and the viral organism is concentrated with a centrifuge. The concentrated material is then collected and additives are mixed with it. The mixture is freeze dried and then this material is milled and sized. This milled and sized materials are then used or stored (See Figure 7.4).

Small-scale use of fertile chicken eggs

The use of fertile chicken eggs as a medium for the growth of viral agents can be used on a small-scale. This type of small-scale production is used in University-type laboratories. Thus, the expertise for this type of processing is widely available.

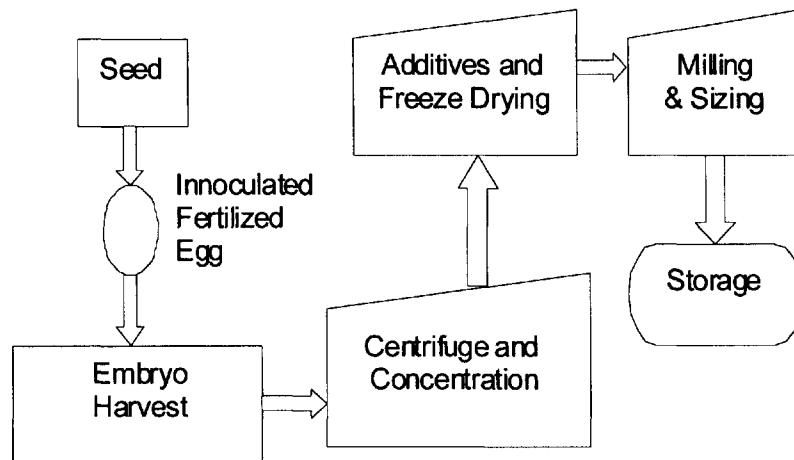


Figure 7.4 Production of viral agents with fertile chicken eggs.

Live Tissue

Live tissue may be used for bacteria as well as viral production. The mechanism for the use of live tissue is analogous to that of viral production with fertile chicken eggs (See Figure 7.5).

Small-Scale Use of Live Tissue

It is feasible to use live tissue to grow biological organisms on a small-scale. For example, *Francisella tularensis* (tularemia) can be grown on blood agar plates. Blood agar is a common material used in high school biology laboratories and is widely available. Each plate is capable of producing thousands of organisms.

Live Animals

Live animals can be used to grow both viral and bacterial organisms. The method of using live animals is similar to the use of chicken embryos and live tissue (see Figure 7.6).

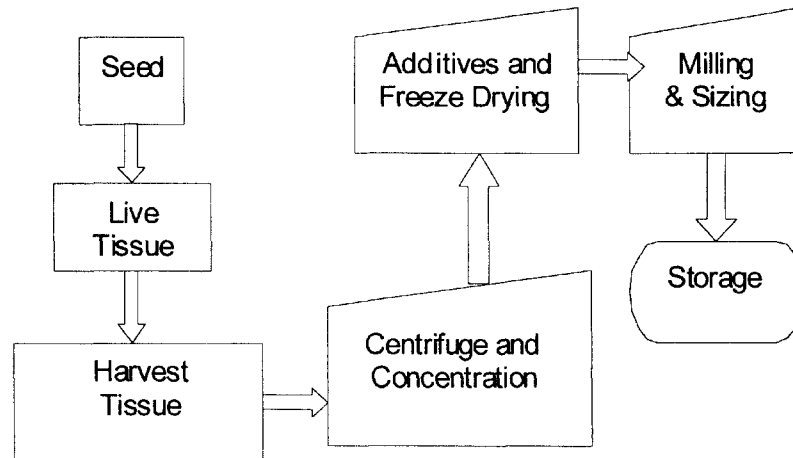


Figure 7.5 The use of live tissue in the growth of biological agents.

Small-Scale Use of Live Animals

Live animals are easily obtained and can be used virtually undetected as a means of incubating lethal biological organisms. Such an operation could occur in a rural as well as an urban environment.

An example of the use of live animals for the production of lethal organisms would be the inoculation of a sheep with anthrax. The sheep would serve as a host for the growth and production of anthrax. When the disease has nearly run its course, the sheep could be killed and the anthrax-bearing tissue harvested for concentration and drying.

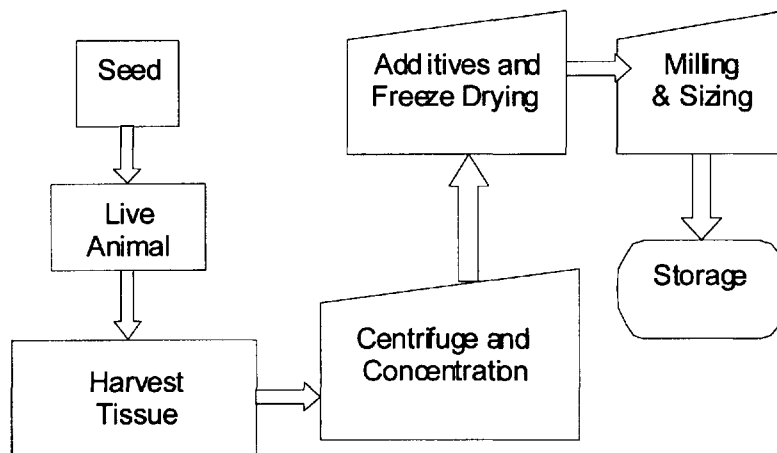


Figure 7.6 Use of a live animal for the production of biological agents.

CONCLUSIONS

Four methods for the production of biological agents were discussed in this chapter: fermentation, fertile eggs, live tissue and live animals. The use of these methods on a large-scale for the production of biological weapons is very difficult to detect, since these same methods are employed by the legitimate vaccine and pharmaceutical industry. This is why the implementation of the Biological Weapons Convention is so difficult [3]. In order to detect the production of biological weapons, it would require detailed inspection of vaccine or pharmaceutical production facilities in a signatory country. Since biotechnology and the pharmaceutical industries use proprietary technology and keep trade secrets, the open inspection of these industries could have important strategic and economic consequences. For example, economic espionage, the theft of trade secrets, costs the United States two hundred and fifty billion dollars per year. The FBI has recently identified 23 countries involved in this practice and the pharmaceutical industry is one of the main targets. Thus countries are not motivated to employ the strict inspection regime that the Biological Weapons Convention would need to become successful.

The only currently available means of addressing the proliferation of biological weapons is through the Australia Group, an informal organization of 30 members. The Australia Group is committed to ensuring that the export of materials and equipment useful for the production of chemical and biological weapons from the member countries is curtailed [4].

To make matters even more interesting, each of the production methods described in this chapter is adaptable to small-scale production and is virtually undetectable. Advancements in biotechnology will only enhance the access to new and more lethal organisms.

In the view of the author, biotechnology will present a more dangerous and complex non-proliferation problem than any other technology for the production of weapons of mass destruction.

REFERENCES

1. K Alibek. Biohazard. New York: Random House, 1999.
2. G Bozheyeva, Y Kunakbayev, Y Yeleukenov. Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future. Monterey Institute of International Studies, Center for Non-Proliferation Studies, <http://cns.miis.edu/pubs/opapers/op1/index.htm>, June 1999.
3. BWC (Biological Weapons Convention). Washington, D.C., U.S. Department of State, 1972. (<http://www.state.gov/www/global/arms/treaties/bwcl.html>).
4. AG (Australia Group), Fact Sheet Released by the Bureau of Nonproliferation, Washington, D.C., U.S. Department of State, April 1, 2000. (http://www.state.gov/www/global/arms/bureau_np/000401_ag.html).

General References

Center for Defense and International Security Studies (CDISS),
<http://www.cdiss.org/cruise1.htm>, 2000

GW Christopher, TJ Cieslak, JA Pavlin, EM Eitzen, Jr. Biological warfare: A historical perspective. *Journal of the American Medical Association*. 6: 412-418, August 1997.

FAS (Federation of American Scientists). Biological Weapons.
<http://www.fas.org/nuke/guide/usa/cbw/bw.htm>.

SM Hersh. Chemical and Biological Warfare. Garden City: Doubleday and Company, Inc., 1969.

Militarily Critical Technologies (MCT) Part II. Weapons of Mass Destruction Technologies (WMD). February 1998. (<http://www.dtic.mil/mctl>).

L Pringle. Chemical and Biological Warfare: The Cruellest Weapons. Hillside: Enslow Publishers, Inc., 1993.

E Regis. The Biology of Doom. New York: Henry Holt and Company, 1999.

US Army 1. Medical Research Institute of Infectious Disease.
<http://www.biomedtraining.org/materials.htm>, 2000.

US Army 2. The Army Tactical Missile System. Special Text 6-60-30.
www.army.mil/gunnery/manuals/afom/afom.doc, 2000

RD Walpole. Intelligence related to possible sources of biological agent exposure during the Persian Gulf war. <http://www.gulflink.osd.mil/library/43917.htm>, 2000.

8

Agroeconomic Bioterrorism

Keith A. Hickey

University of Missouri, Columbia, Missouri

INTRODUCTION

Agroeconomic bioterrorism is bioterrorism conducted against economic and agricultural commodities such as animals/livestock, food crops and other derivative products and systems (e.g., cotton, wool, leather, milk, wood, food distribution systems, etc.). Since the attacks are not conducted against people directly, the desired effects are economic damage which requires a widespread geographical consideration. We care about 100 people; we don't care about 100 animals, 100 trees, 100 food plants, etc. Agroeconomic targets are systems involving complexity and are widespread in scope. Local (focal) or point attacks can cause significant economic damage, primarily through psychological or societal reactions to the perception of risk and danger. Distributed (or multi-focal) attacks on the agroeconomic base of food crops or animal livestock require both similar and significantly different considerations than do bioterrorism or biowarfare directed at people. The response to agroeconomic bioterrorism is by necessity multi-disciplinary involving

- Spatial-temporal analysis of relationships (systems theory, operations research, and spatial econometrics).
- Environmental biophysics for the physical propagation of toxins and pathogens in water, dust or air (soil science, hydrogeology, aerosol microphysics, and meteorology).

- Epidemiology and disease propagation modeling (plant pathology, veterinary medicine, entomology and demography).
- Information and communication systems (geographical information systems, common databases, communication and reporting networks or pathways).

U.S. agro-economic system has a dedicated system of expert and professional response to naturally occurring plant and animal diseases and pests known as the Animal and Plant Health Inspection Service (APHIS) of the United States Department of Agriculture (USDA). Specialized research capabilities are available through the USDA Agricultural Research Service (ARS). Bioterrorism and biowarfare against agro-economic systems would activate these teams to respond in a manner similar to naturally occurring outbreaks. In fact, often the difficulty is in recognizing a deliberate attack and the identity of the attacker as opposed to a spontaneous outbreak. The teams of the APHIS are highly trained and are experienced with responding to naturally occurring threats to the agro-economic system. "The Veterinary Services (VS) unit has an Emergency Programs staff which coordinates efforts to prepare for and respond to outbreaks of exotic animal diseases. The staff is assisted in its efforts by Federal and State field veterinarians, animal health technicians, and disease specialists." (APHIS web page www.aphis.usda.gov). In addition, the National Animal Health Reporting System (NAHRS) is a joint effort of the U.S. Animal Health Association (USAHA), the American Association of Veterinary Laboratory Diagnosticians (AAVLD), and the USDA APHIS. The NAHRS is voluntary and considered to be one part of a comprehensive, integrated animal health surveillance system in the U.S. (APHIS web page www.aphis.usda.gov).

Similarly, the Plant Protection and Quarantine (PPQ) unit of APHIS has the responsibility regarding outbreaks of plant diseases. "The American plant safeguarding system is focused on preventing the entry and establishment of invasive plant pests in the form of insects, plant diseases, noxious weeds, and other injurious organisms." (Safeguarding American Plant Resources, USDA-APHIS-PPQ July 1, 1999). "The USDA-APHIS battles invasive species along multiple fronts at any given period. During the 1997-1998 period, no less than 20 introduced plant pests (usually near ports of entry) were the targets of eradication campaigns, strict quarantines, or regulatory actions by the USDA. Additionally, several animal diseases were targeted for management or eradication. As opposed to accidental invasions, the intentional introductions of exotic invasive species may differ in the following ways: (1) use of non-traditional pathways, (2) increase of the probability of survival of the pest in-transit, (3) widespread dissemination of the disease from disparate foci, (4) use of highly virulent strains, (5) high rates of inoculum, (6) introduction into remote areas, (7) targeting of susceptible natural environments, (8) release of multiple species simultaneously, and (9) precise timing of releases to coincide with maximal colonization potential" [1].

In addition to foreign terrorists or enemies who are interested in the destruction or economic disruption of the U.S., there are dedicated domestic eco-terrorist groups such as the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF) whose principle call to arms and agenda is the disruption of the U.S. agribusiness system (Richard Berman, "Enemies here threaten food," USA Today Nov. 1, 2001). For a further discussion, see the following Psychological and Economic Terrorism section as well as the two case studies on Genetically Modified Organisms (GMO) and Hoof and Mouth Disease (HMD).

"Since the September 11, 2001 attacks, all USDA personnel at U.S. at ports of entry, food inspection facilities, and research labs and buildings, are currently on a heightened state of alert. At ports of entry, personnel are conducting intensified product and cargo inspections of travelers and baggage to prevent the entry of animal or plant pests and diseases." "We are examining our responsibilities – looking at our short and long term needs to ensure USDA continues to protect America's food supply and agriculture against pests and disease of any kind," says Agriculture Secretary Ann M. Veneman. "We stand ready – and are making sure that we are prepared, coordinated, and able to respond should we ever face an emergency" ("Agricultural Biosecurity," USDA Q&As 10/25/01).

"The feasibility of an agro-economic attack hinges on three factors:" [2]

1. The technical ability to acquire and deploy a bioagent.
2. An interest in sickening or killing animals or crops as a means to its goal.
3. A desire to do so using the bioagent.

AGROECONOMIC SYSTEMS AND VULNERABILITIES

Point Attacks on the Food Supply Chain

Attacks on the food supply chain can be from many sources including poisons, toxins, or contaminants of a biological, chemical, or radiological nature. Point attacks on centralized facilities involve considerations of access and biosecurity. Crop-dusting planes as dispersal units of biological or chemical agents, insertion of cyanide into drugs such as Tylenol, contaminating food processing plants, and anthrax-contaminated letters are examples of point attack vulnerabilities. Surveillance and inspections, access control, sophisticated packaging, automated handling systems, food and mail irradiation to kill microbes, and other local biosecurity measures [3] to prevent security breaches and the introduction and movement of infectious diseases or toxins can reduce the risk of point attacks.

Distributed Attacks on the Agroecosystem

In contrast, distributed attacks on the agroecosystem would not typically involve chemical or radiological contaminants because of dispersal issues for large areas. Biological agents would be the terrorist weapon of choice to cause a widespread economic disruption. Biosecurity involving access control becomes difficult to impossible to implement because of the size and the scope of the agribusiness industry which is primarily conducted in rural areas. An attack on the more than \$200 billion per year agriculture industry with its open fields and crowded feedlots would be relatively simple to conduct (Anita Manning, USA Today, Oct. 2001). Given the difficulty in implementing security, a widespread attack, especially in food crops, is not as easy to conduct as it would appear because of the natural barriers in crop disease propagation, and the rapid response and disease containment provided by plant pathologists in commercial crops, and animal health inspectors and veterinarians in commercial livestock.

“It has been known for a long time that many naturally occurring microorganisms and toxins are potential biological weapons against people, and crops with many examples of deliberate infections or infestations including rinderpest virus in cattle, glanders and anthrax in horses, African swine fever virus and the Colorado potato beetle.” [1]. Plant diseases as bioweapons such as rusts, blight, smuts, etc. were also heavily studied in the former Soviet Union as were easily transmissible animal diseases such as hoof and mouth disease, rinderpest, and African swine fever. As many as 10,000 Soviet bioweapons researchers at the Soviet Union’s Biopreparat were working solely on anti-agricultural bioweapons projects [1]. The New York Academy of Sciences Volume 894 *Food and Agricultural Security: Guarding Against Natural Threats and Terrorist Attacks Affecting Health, National Food Supplies, and Agricultural Economics* [1] is the most complete detailed survey of potential bioterrorist threats against the U.S. and the world agricultural systems.

Descriptions of the Plant/Animal Disease Process

Plant Pathology is the study of plant disease. Veterinary Medicine is similarly related to the study of animal disease. “Disease is the result of a dynamic interaction between an organism (plant, animal, or human) and its environment. This interaction results in abnormal physiological and often morphological or neurological changes in the organism. The expression of a disease by a host is called a symptom. The actual visualization of the pathogen is called a sign. Signs and symptoms relate to the presence of a disease. One characteristic that all symptoms share is that some aberrant function, growth pattern, or physiological dysfunction affects the well-being of the organism. Therefore, disease may occur at any level of organization within an organism.

There are four elements in the propagation of disease – a susceptible host, a virulent pathogen, a favorable environment and the amount of time under consideration. Most disease problems are caused by biotic pathogens or living agents.

These agents include viruses, mycoplasmas, bacteria, fungi, protozoa, nematodes, and parasites. The term environment is general and includes obvious factors such as temperature, moisture, etc. as well as interactions between the pathogen and other competing microorganisms (the biological environment). The cause of disease need not be restricted to infectious agents, such as viruses, bacteria or fungi, but may also be caused or enabled by nutritional or genetic disorders." (Wyllie, Thomas D., Plant Pathology Course Notes, University of Missouri-Columbia ©1995). In the case of bioterrorism against commercial plants and animals, the health status and environmental conditions of the organism involved radically affect the degree of success of the bioattack.

PSYCHOLOGICAL AND ECONOMIC TERRORISM

The Psychology of Terrorism and the Terrorist

The psychology of agroeconomic bioterrorism has some significant differences to the psychology of either warfare or the use of weapons of mass destruction in terrorist attacks against human targets. While all terrorism attacks are short term tactical missions against limited targets conducted with a longer range strategic goal of government destabilization or motivating societal or policy changes, agroeconomic bioterrorism can instill the same desired fear, panic and loss of confidence without the direct loss of human life. In fact, the long-term effects and psychological damage inflicted by an agroeconomic attack might be significantly greater because of long lasting and more widely distributed economic hardships without the natural national anger and sense of purpose often generated by the loss of human life.

The only effective antidote to the psychological effects of bioterrorism is knowledge through familiarization, education and training, and the perception, confidence and reality of governmental expertise and ability to deter future attacks and restore the country to health and normalcy in a reasonable time frame. The psychological effects of terrorism is the perceived loss of power and control by both the individual and the government to protect themselves.

"Because it is effective and cheap (and sponsorship can be disguised or denied), terrorism increasingly will be a weapon of choice for extremists and rogue states. Whereas politically motivated terrorism appears to be in decline, terrorism carried out in the name of religion is increasingly ascendant. Religious zealots exhibit few self-imposed constraints" [1]. Eco-terrorism is a form of religious zealotry and extremism with the worship of "Mother Earth".

"Terrorism is an act composed of at least four crucial elements." [4]

1. An act of violence against plant, animal or human.
2. A motive or goal.

3. Perpetuated against innocent persons.
4. Staged to be played before an audience whose reaction of fear and terror is the desired result.

The categories of persons who commit terrorism are criminals, crusaders and crazies [5]. The profile of an agro-economic bioterrorist would likely fall into the crusader category except when done by state-sponsored terrorism. Attacking crops, animals and economic commodities does not cross the potential barrier to killing humans. Although personal gain could be a motivation, it is much more likely that idealism with a desire for prestige and recognition within a collective cause is the most likely motivation.

An example is the eco-terrorist movement including the Earth Liberation Front (ELF) and Animal Liberation Front (ALF), which have recently conducted many violent and destructive acts including arson and vandalism especially in the states of Oregon and Washington (Bourrie, Sally Ruth, Boston Sunday Globe, July 22, 2001). By destroying property only, the group regards their work as “non-violent, direct actions”. Acts have been committed against logging, agriculture and animal research.

“The motivations for agro-economic bioterrorism can include:” [2]

1. The profit motive such as commodity speculation.
2. Anti-GMO (genetically modified organisms) or other eco-terrorist extremist idealism.
3. The psychological barrier is often lower when the target is animals, plants, or economic as opposed to the taking of human life.
4. Agricultural targets are “soft targets” with relatively low security, easily attacked with limited financial or technological resources, and hard to detect and prosecute the attacker.

Economic Terrorism

Past incidents of large-scale disease outbreaks show the financial impact of an outbreak includes not only the cost of the lost agricultural products, but also the cost of the disrupted trade, and even societal change and instability [2, 6] “For any fool-proof system, there is a fool who is bigger than the proof,” (Edward Teller, 1980, University of Missouri-Columbia College of Engineering Croft Lecture). These words show the basis of insurance in the world of business. Insurance rates are the price of risk as estimated from current assumptions and future predictions of economic conditions, wars, natural disasters and terrorism. In rapidly changing times and with risk uncertainty, insurance companies will raise their premiums for coverage or will back away from insuring the risk until predictability returns.

Risk to the insurers and liability vulnerability to natural or man-made disasters is spread among the various insurance companies by a process of reinsurance. Terrorist attacks on Sept. 11, 2001 and the following anthrax bioterror attacks

have significantly raised the uncertainty of insurance risk estimates leading to upheavals in the property and casualty insurance of businesses and difficulties in the reinsurance industry. "Without terrorism coverage, real estate development, manufacturing, and transportation could be effectively shut down," (Mike McNamee, Business Week, Dec. 10, 2001). Banks to date have not started pulling loans due to commercial properties being denied terrorism coverage; however, banks have been reluctant to finance new projects until Congress acts on the issue of terrorism insurance (Christine Dugas, USA Today, Jan. 10, 2002).

A study on the economic impacts of the September 11, 2001 attacks yielded ten tentative conclusions [7]: Relevant conclusions for this presentation included:

- An increased unemployment rate and decreased Gross Domestic Product (GDP) trend.
- Diffusion of the decrease in activity in one sector of the economy (e.g., airline, travel) into other sectors of the economy more rapidly than in past recessions.
- A consumer confidence decline with decreased consumer spending increasing the probability and possible severity of a recession through early 2002, higher oil prices not likely to be a major problem unless military or terrorist actions disrupt oil supplies.
- Increased probability and possible severity of a recession in most other nations, especially major U.S. trading partners, such as Canada and Mexico, as well as the U.S.
- Unlikely to have a major impact on agricultural prices in the short run, however, an international recession would reduce the demand for U.S. exports and could result in downward pressure on agricultural prices.
- The U.S. and other major nations must use lower interest rates, increased government spending, or decreased taxes to encourage economic growth. The effectiveness of lower interest rates may be very limited.

It is clear that acts of terrorism through both actual economic assault and perceptions of risk can have magnified effects throughout the U.S. and the rest of the world through complex economic relationships of consumer confidence and the global trade and finance markets.

THE AGROECONOMIC PROTECTION AND RESPONSE HIERARCHY

"The threat of an agroterrorist attack can be countered on four levels:" [2]

1. At the organism level, through animal or plant disease resistance.
 2. At the farm level, through facility management techniques designed to prevent disease introduction or transmission.
-

3. At the agricultural sector level, through USDA disease and response procedures.
4. At the national level, through policies designed to minimize the social and economic costs of a catastrophic disease outbreak.

Kohnen's paper [2] discusses in depth the threat of agroterrorism and a comprehensive strategy to counter it. "The Office International des Epizooties (OIE), also called the World Organization for Animal Health, is an intergovernmental organization with 155 member countries. The OIE maintains a list of transmissible diseases which have the potential for very serious and rapid spread, irrespective of national borders, which are of a serious socioeconomic or public health consequence and which are of major importance in the international trade of animals and animal products. List A diseases could severely damage the U.S. agricultural market, since an outbreak of one of these diseases is internationally recognized as grounds for export embargo" [2]. An example of a List A animal disease is HMD.

"Vaccines exist for most of the List A diseases, though they are not generally used except to control an emerging outbreak. Vaccines can keep animals from acquiring diseases, but in most cases they do not keep animals from being carriers. A cow vaccinated against HMD can carry the disease in her throat tissues for two and a half years after exposure. Also, a vaccinated animal cannot be distinguished from an infected one; the titers are the same" [2]. An even more sobering thought is the spread of the HMD into the wildlife population, such as deer, where population numbers have skyrocketed in recent years. An effort to eradicate the disease epidemic in both the commercial livestock bases of pigs, cattle and sheep as well as the deer population could reach monstrous level. This is why the genetic efforts in vaccine production and vaccine quality is so exciting. Incorporating a vaccine into both a feed plant for animal food-stock and into forage crops for the wildlife would be critical. In addition, it would be beneficial to have a vaccine available where the titers for infected and vaccinated animals could be easily distinguished.

"Comparable to the OIE for animal export guidelines, the International Plant Protection Convention (IPCC) sets international standards for plant export guidelines. The IPCC has 111 member countries, each of which submits its own plant import restrictions" [2]. "Plant pathogen resistance include herbicides, to eliminate weeds, and pesticides, to control insect pests. Virus-resistant plant varieties reduce the need for insect control as a means of stopping virus transmission" [2].

At the farm level there is excitement (and fear) in genetically modified organisms (GMO) or biotech crops. Biotech methods may rapidly create new resistant crops that significantly increase crop yield with a reduced cost in herbicides and pesticides, and without the laborious Mendelian plant breeding initiatives that have previously increased crop yields. Unfortunately, there are concomitant concerns with genetic diversity from the resulting monocultures, food quality, etc. that

have lead to controversy, both within the agricultural industry between farmers and agribusiness, between countries and with environmental activist groups.

“In animal production at the farm level, intensive farming of livestock animals and broilers is efficient; it allows farmers to raise more animals with fewer resources. The increased density of animals per farm heightens the epidemiological risk. The trend toward larger farms is unlikely to change in the foreseeable future” [2].

“At the sector level, there is the USDA disease detection and response mechanism. The organization and duties of APHIS were previously discussed. A detection/surveillance system using satellite tracking systems (remote sensing) for crop distress is being developed by ARS. By combining various field measurements such as reflectance with Global Positioning System (GPS) information, the system (in reality a Geographic Information System – GIS) can pinpoint problems within fields. This system provides a rapid response and integration of available information concerning crop diseases and crop stress” [2]. The technology and beneficial applications of remote sensing and GIS will be discussed in more detail in a later section.

Similarly, the sector response to animal diseases needs rapid diagnostic capabilities. Some of the state-of-the-art genetic tests and diagnostic detection technologies will be discussed in a later section.

At the National level, the USDA as well as other Federal Agencies have the responsibility to eliminate the perception of risk as well as the actual risk. The study of perceived risk, and the psychological and public relations implications have a long and interesting history [8, 9]. Often, Federal “deep pockets” are the most essential element in rapid eradication of the threat and compensation to the directly economically injured.

TECHNOLOGIES IN AGROECONOMIC TERRORISM PLANNING AND RESPONSE

Bioterrorism Detection and Analysis

The general identification methods of bioagents from either bioterrorism or biowarfare include [4]:

1. Isolation of the etiologic agent by culture (possible in one to two days for some agents).
2. Detection of toxin by mass spectroscopy, animal inoculation, or other methods.
3. Antibody detection (specific immunoglobulin M, IgM, may appear within 3 days).
4. Antigen detection via enzyme immunoassay or other sensitive assay methods.

5. Genome detection employing DNA probes.
6. Detection of metabolic products of the infectious or toxic agent in clinical specimens.

“Detector systems and methodologies are rapidly evolving and represent an area of intense interest within the research and development community. The principal difficulty in detecting or remote sensing of bioagent aerosols stem from differentiating the artificially generated bioagent cloud from the background of organic matter normally present in the atmosphere” [10]. The key problems in laboratory-grade diagnostic detection is the cost, portability, complexity, sensitivity, specificity and speed of diagnosis. Modern biotechnology approaches have made significant progress in the detection of bioagents.

“Polymerase Chain Reaction (PCR) is a fast, inexpensive technique for making an unlimited number of copies of any piece of DNA. Sometimes called molecular photocopying, PCR has had an immense impact on genetic research. The powerful duplication ability of PCR allows genetic and molecular analysis using small amounts of cells or tissues” [11]. “Sequencing uses DNA polymerase (an enzyme) to synthesize a complementary copy of the target DNA. The polymerase extends, in the 5’ to 3’ direction (directional ends of starting and stopping), a short segment of DNA (known as a primer) that has to be annealed (joined) to the 5’ end of the target sequence to initiate the process” [12].

“A DNA marker is simply a uniquely identifiable segment of DNA. Markers can be thought of as landmarks, and a set of markers whose relative positions (or order) within a genome are known comprises a map. PCR-based markers are commonly referred to as sequence-tagged sites (STS). An STS is defined as a segment of genomic DNA that can be uniquely PCR amplified by its primer sequences. STS markers may be developed from any genomic sequence of interest (e.g., bioagent). Polymorphic markers are those that show sequence variation among individuals. A type of polymorphism detected by PCR-based analysis is a single nucleotide polymorphism (SNP), which results from a base variation at a single nucleotide position. SNPs lend themselves to highly automated fluidic or DNA chip-based analyses and have quickly become the focus of several large-scale development and mapping projects in humans and other organisms” [29].

DNA-based computer chips are being developed to detect and identify biological pathogens to begin to address the issues of rapid diagnosis and wide specificity and sensitivity (Moore, Samuel K., “Making Chips” IEEE Spectrum March 2001, pp. 54-60). DNA microarrays are used to study gene activity or expression, and diagnose diseases. Gene expression shows the subset of genes in a cell actively making proteins. These researchers have adapted existing tools — semiconductors, inkjet printers, and flat panel displays — to the manufacture of these DNA microarrays. Active electronic elements in the microarrays are used to manipulate and sense DNA. Microarrays can perform experiments with thousands of genes simultaneously

Military as well as civilian development of fast, portable bioagent detectors (Christopher Aston, "Biological Warfare Canaries," IEEE Spectrum, Oct., 2001 pp. 35-40) has been very active. Detectors can be based on different technologies including DNA-based detectors, mass spectrometry, antibody-based tests and sensing of chemicals and bacteria using indicators and synthetic compounds that change state when exposed.

Now that various genomes have been sequenced (Human-34,000 genes), the new game is proteomics-study of the proteins (Human – 500,000-1 million proteins) which increases the computational and database organizational demands by more than three orders of magnitude (Begley, Sharon, "Solving the Next Genome Puzzle," Newsweek 2-19-01). This level of data demands even more automation using the tools of microchips and large scale computation resources.

Geographic Information Systems and Remote Sensing Technology

A Geographic Information Systems (GIS) is a combination of computer technologies that integrate massive databases of spatial data, and provides a display and query interface for building and analyzing spatial relationships. GIS uses geography and computer generated maps as an interface for integrating and assessing massive amounts of location-based information [13]. On the ESRI ArcUser site www.esri.com applications of GIS have been developed for public safety, disease tracking and emergency response that allows public safety personnel to effectively plan for emergency response, determine mitigation priorities, analyze historical events and predict future events. GIS can also be used to get critical information to emergency responders upon dispatch or while on route to an incident to assist in tactical planning. Spatial-temporal analysis can improve organizational integration of data and information allowing better decisions based on time and spatial relationships as well the visualization of data. GIS can manage and portray spatial data for epidemiological modeling of disease diffusion in a susceptible population in space and time, as well as overlaying biometeorology influences of stresses of heat and weather, soil type, topology, etc. [14].

In emergency response situations quick and accurate information is the key. Also, flexible systems are needed to respond to new, unexpected threats. Integrated comprehensive databases and communication networks are essential. Breakdowns in uniform response and coordination between separate responder units and organizations are the first casualty of information and decision support systems that are not properly designed.

A draft report "Implementation of Recommendations for Using Geographic Information Systems in APHIS" is available on the APHIS web site www.aphis.usda.com. Its first recommendation is "GIS should be recognized as an important methodology in the way APHIS does business". On the same web site, the Center for Animal Disease and Information and Analysis (CADIA) has a link to Analysis Information with GIS and Spatial Analysis for Geospatial Analysis.

Remote sensing obtains data from a sensor at a distance remote from the measured phenomena. Usually, the data measured from the sensor are from the electromagnetic radiation spectrum either directly, or indirectly, from reflection or reradiation. The electromagnetic spectrum measured can include light, thermal (heat), radar, etc. or a combination of the various EM spectrums or bands to provide a multi-spectral composite image [15, 16]. "Remote sensed data can be collected using either passive (only receive a signal) or active (send/receive signals) remote sensing systems. Suborbital (airborne) and satellite remote sensing systems can provide fundamental biological and/or physical (biophysical) information directly, without having to use other surrogate or ancillary data" [16]. Remote sensing imaging capabilities and data processing include image interpretation and analysis, classification methods, morphological function and elevation modeling and transformational analyses. These biophysical parameters can be used in a site-specific environmental biophysics analysis [17].

Given an environmental dataset geo-referenced in a GIS, spatial statistics can be performed for an understanding of spatial processes and an investigation of the important spatial statistical variable of spatial autocorrelation. Spatial statistics can be used to characterize and identify differences in variables across space and their significance in quantitative geography [18-21]. When observations are irregular in time space, the variogram sample estimator can be used to estimate spatial variance. There is relation between the variogram and the autocovariance function [18, 21]. A good introduction to the concepts and utilization in practice of spatial statistics is given in references 19 and 21.

The integration of physical data obtained from remote sensing systems including GPS within a GIS framework can be critical to advancements in plant breeding field trials evaluating crop yield and resistance. "A central problem confronting a plant breeder when comparing genotypes in a field trial is that the yield of a genotype is markedly affected by the condition, particularly the soil moisture and fertility, of the plot in which the genotype is sown. Comparison problems increase with separation between plots and lead to the conclusion that marked soil variations occur which tend to make adjacent tree or plot yields alike. This has major repercussions in the replication and randomization statistics in agricultural field trials. The non-uniformity of conditions over the trial is sometimes referred to as within-trial heterogeneity or 'fertility' trials. Heterogeneity or fertility trends result in spatial correlation between plots, so a useful statistic for examining the within-trial heterogeneity is the spatial autocorrelation coefficient" [22]. "The main purpose of spatial analysis is to estimate genotypic effects and their standard error of differences. Resulting estimates of genotype effects from spatial analysis to reduce variability showed increased precision as the within-trial heterogeneity increased compared to standard incomplete block analysis" [22].

"For plant breeders, the strength of a GIS system is its capacity to provide information on test locations that can be used in supporting the analysis of genotype x environment interactions. For example, temperature, relative humidity, dewpoint and dew duration, and wind direction and velocity all have important

and direct influences on plant disease epidemiology. Recent insights into the relationship between meteorological conditions and disease intensity allow simulation (using long-term meteorological records) of the intensity and frequency of specific diseases or, in some cases, disease vectors (e.g., insect carriers). Mapping the extent and intensity of crop diseases allows characterization of test locations, as well as production areas. Characterization of production areas assists in the setting of research priorities. A GIS can provide temporal (frequency/intensity) and spatial information supporting research efforts" [22]. Similarly, real-time remote sensing data from satellites is available for input to a GIS for use by natural resource managers such as precision agricultural professionals, who will use the data to more accurately determine what portions of land received precipitation and determine where best to apply agricultural chemicals.

Time Series Analysis and Risk Assessments

Most time critical decisions or strategic predictions are not made in an environment of absolute certainty, but are instead made with incomplete information and involve statistical analysis or estimates of the current state or predicted future state of a system. The National Plant Board (NPB) in its recommendations to the USDA APHIS stated "The pest risk analysis process should be continuously improved, expanded, and implemented. The quest for efficiency and transparency requires development of pest risk analysis models that incorporate and standardize levels of information needed to perform the risk analysis. Cost-Benefit analysis models should be used to incorporate social sciences and economic theory into the risk management process" [23]. Techniques of risk analysis and risk assessment have long been used in the aerospace and nuclear technology industries [24, 25]. Preliminary Hazards Analysis (PHA), Event Tree Analysis (ETA) and Fault Tree Analysis (FTA), and Consequence Analysis (CA) have been used to identify accident sequences and describe the consequences of the accident.

Specialized environmental risk assessment methodologies have application in the context of bioterrorism risk assessment especially in the environmental transport of diseases and toxins. Previous work has been done in aerosol transport, environmental and food pathway transport of radionuclides, pollution studies, and soil transport of contaminants [26-33].

In addition to the standard risk assessment and analysis, the issues of measurements and estimates made over time and space have been studied in the context of time series analysis. Standard analysis of variance (ANOVA) and regression analysis techniques contained in common statistics packages such as SAS, SPSS, S-PLUS etc. for providing estimates and accessing the sources of variability [34] have to be expanded or modified in the case of time series analysis [18, 35]. S-PLUS has built-in time series analysis algorithms as well as being extensible with its built-in matrix processing. SAS and SPSS have routines that perform basic time series analysis, SAS/ETS and SPSS Trends. For the case of multivariate time series analysis, a matrix approach is absolutely necessary [18, 35].

For cost-benefit analysis, economic and financial relationships and quantities that vary in space and time, and have spatial-temporal correlation are studied in the context of econometric and spatial econometric analysis of time series. Econometrics and spatial econometrics often has some specialized characteristics and assumptions that differ from standard time series analysis [36, 37].

Bioterrorism Response Modeling and Bioinformatics

Information quality and uniformity is critical in emergency planning and emergency management response. Different data sources (e.g., data acquisition from satellite sensors such radar, thermal, GIS, GPS) often have different datasets measuring some but not all of the same parameters and with various degrees of accuracy. Information from various sources both in time and space can be integrated (fused) into a single database with a combined accuracy superior to any one single dataset. This process is called Multiple Sensor Integration (MSI) or Multisensor Data Fusion [38] and has been highly developed in the military as part of situation awareness, especially for tactical aerospace state estimation in target tracking and for decision support systems. Classical and modern techniques for analyzing signals include Fourier spectra, statistical properties of time series, correlation functions, spectral density functions, and time series modeling [39].

Likewise, Bioinformatics seeks to make sense of a bewildering amount of data through computational and database techniques. "Biology in the 21st century is being transformed from a purely laboratory-based science to an information science as well. The information includes comprehensive global views of DNA sequence, RNA expression, protein interactions or molecular transformations. Increasingly, biological studies begin with the study of huge databases to help formulate specific hypotheses or design large-scale experiments. In turn, laboratory work ends with the accumulation of massive collections of data that must be sifted. These changes represent a dramatic shift in the biological sciences" [12].

"As molecular biology works towards characterizing the genetic basis of biological processes, mathematical and computational sciences are beginning to play an increasingly important role: they will be essential for organization, interpretation, and prediction of the burgeoning experimental information" [40]. These mathematical and computational sciences include:

- Object-oriented computer languages for information parsing and pattern matching in DNA sequences such as Perl, Bioperl or Scheme [12, 41, 42].
- Data-mining techniques [43] involving database construction issues as well as multivariate statistical analysis (principal components, factor analysis, etc.) and decision making [18, 44].
- Categorical time series analysis [18] for estimating the spectral envelope of a DNA sequence using the nucleotide alphabet to find coding and non-coding signal segments.

- Mathematical and statistical genetic analysis such as linkage analysis to map genes and computational methods to predict protein structure which is critical for the protein function [40, 45].

To make sense of this overwhelming amount of a data, a user-friendly human interface to the various databases is needed. Also, in a rapidly changing technology environment, this human interface should be able to be easily modified to incorporate and investigate new paradigms of computation and new algorithms, i.e., the interface should be a rapid prototyping system. Because of the highly multidimensional characteristics of the data and the necessary algorithms to process it, the interface should include at a bare minimum embedded or easily added vector and matrix operation constructs. Several processing environments include these capabilities including S-PLUS, Mathematica, Matlab, etc. Mathematica [46, 47, 48], and S-PLUS [49, 50, 28] are two of the most useful for processing interfaces to large databases such as generated in GIS, remote sensing and bioinformatics.

A discussion of Mathematica as a front-end user interface to a GIS database and rapid prototyping system will be given. Mathematica is a programming language as well as a comprehensive symbolic computation system. As a higher level language, projects developed using the resources of Mathematica can be developed much quicker than similar projects using FORTRAN or C, albeit with a computational overhead and reduction of computational speed. Mathematica inherently contains several characteristics that aid programming in the rapid prototyping environment including [48]:

- Mathematical formula and algorithms.
- Pattern matching capabilities.
- Simple manipulation of structured data (lists, vectors, matrices).
- Modularization for organizing larger programs.
- Object-oriented elements to make code development easier.
- Traditional procedural programming in the style of FORTRAN and C.

These elements, in addition to built in graphical and display tools allow the rapid development of processing algorithms to control the large GIS system with its massive database and allow the interface processing and display of the desired data. This kind of system would be a significant aid in the optimized use of GIS data for modeling and emergency response.

CONCLUSIONS

Agroeconomic bioterrorism is a real threat in the present world. The agroeconomic system in the U.S. is large, diverse and of critical economic importance. It has both inherent safety mechanisms and dangerous vulnerabilities. The USDA

and the U.S. agricultural response system (APHIS and ARS) of plant pathologists, veterinarians, and other professionals are under-funded and under-staffed for the magnitude of the threat that they face – both natural occurring pests and diseases as well as threats deliberately introduced. However, they have real-world experience and procedures dealing with natural disease outbreaks in plants and animals.

The agricultural system is relatively unprotected, but a bioterrorist would have to attack the agricultural system over a wide geographical area and coordinated with an assault on many different plant and/or animal systems to have a truly devastating effect on the diverse U.S. economy. Not impossible to implement for a well-trained, well-funded bioterrorist group, but certainly not trivial for a casual effort.

The anthrax bioattack shows the difficulty in coordinating a dispersed and distributed attack with massive casualties and yet it also shows the relative ease that a bioattack can be carried out to inflict psychological and economic damage much greater and widespread than the real injuries. The September 11, 2001 terrorist attack shows the propagation of economic effects from one economic sector and one geographic location throughout the linked economy to other sectors and other geographic locations. We truly live in a complex global and networked economy with all the sophistication and benefits that it brings, as well as the potential risks entailed when it fails. The U.S. agro-economic system is a vital and vulnerable part of that global economy.

CASE STUDY 1: GENETICALLY MODIFIED ORGANISMS (GMO)

Genetically Modified Organisms or Biotech crops generate significant passion and controversy between several special interest groups with agendas at several levels. With that passion, comes the motivation for activism, extremism and even eco-terrorism against agribusiness. It is hoped that with perceived adequate regulation and enhanced consumer education that biotech foods will gain acceptance in consumer markets. Resistance to food derived from GMO is especially high in Europe where as many as 80 percent are opposed. The economic and environmental potential benefits for biotech crops are significant with increasing crops yields that will benefit the world food supply, while reducing the environmental assault of large scale use of herbicides and pesticides. The U.N. Development Program (UNDP) agency has come out with a 2001 report in support of biotech foods in the effort to stem world hunger. An example of a GMO is “Golden Rice” that has been modified to contain beta carotene to combat vitamin A deficiencies in Asia that lead to blindness. Opponents such as Bio-Justice that are opposed to genetic engineering have called golden rice a “Frankenfood.”

In addition to biotech food, research in plant-based genetic derived products such as vaccines and human disease therapies are ongoing. These vaccines and therapies have the potential to create public relations “good will” that may aid the biotech food markets by association.

The most widely noted case of biotech crops generating controversy is in the case of the genetically modified corn known as Starlink. "StarLink had won government approval as animal feed but not as food for humans. It cross-pollinated widely contaminating 430 million bushels of corn, and triggering nationwide recalls of taco shells, corn chips and other foods" (Elias, Paul, "Molecular Pharners hope to raise human proteins in crop plants," AP release, St. Louis Post Dispatch, 10-28-01). This is an example of how significant economic damage can be accomplished through a bioassault without even endangering human life.

Bt corn is another example of a GMO that has been modified using the *Bacillus thuringiensis* to provide natural pest resistance. "Plant genetic engineering refers to the transfer of foreign DNA which codes for specific genetic information, from a donor species into a recipient plant species by means of a bacterial plasmid, virus, or other vector. A segment of DNA that codes for a desirable trait is inserted into the plant genotype where it replicates and is expressed in the new plant genotype. This is similar to the plant breeder backcross method in which desirable genes are transferred to a recipient genotype by a succession of crosses. The difference is that the plant breeder can employ the backcross only among species that are cross-fertile, whereas the molecular biologist is not limited to obtaining the DNA from a donor plant species that is cross-fertile with the recipient plant species" [51]. "The use of Bt corn was developed as a way of providing corn with natural resistance to some pests, particularly the European corn borer and to a lesser extent the corn earworm, the southwestern corn borer, and the lesser cornstalk borer" (Research Q&A: Bt Corn and Monarch Butterflies, Agricultural Research Service, web page www.ars.usda.gov). The use of pesticides with Bt corn was enormously reduced with significant positive environmental benefits. The Bt varieties of corn are currently approximately 20 percent of the U.S. corn crop.

Bt corn has been controversial in the public press because of potential threats to monarch butterflies and possible human allergic reactions. These allegations were refuted in 2001 by studies from EPA and USDA on monarch butterflies, and CDC for the alleged allergic reactions.

The Mexicans have been angered recently that unlabeled U.S. imports had transferred modified genes including the Bt gene to local corn, even though planting genetically modified crops is banned in Mexico. The danger is that genetically modified strains could displace or contaminate the valuable Mexican genetic diversity resource stockpile of wild varieties of corn (Stevenson, Mark, "Accidental spread of modified corn is seen as cultural attack," AP release, St. Louis Post Dispatch, 1-1-02). Genetic diversity is an important issue for plant breeding and evolutionary adaptation [52, 53]. Diversity is essential for species survival in space and time, by adaptation to specific environments. Genetic diversity has a leading role in competition, symbiosis and parasitism, impact of climate, absorption of nutrients and the effect of nutritional deficiencies. The importance of wild relatives for breeding is important for the improvement of crops by wild genes for disease and pest resistance. One advantage of gene transfer through genetic engineering is by opening up tertiary (distantly related) gene pools [52].

The only thing certain is that controversies associated with GMO will continue for the near future. It is in the political agenda of certain environmental activist groups to continue the hysteria of imagined threats while ignoring the benefits associated with biotech foods. Real problems should be addressed as they come along (which they always will in the real world) with a rational and thoughtful analysis backed with technical expertise.

CASE STUDY 2: HOOF AND MOUTH DISEASE (HMD)

Hoof and mouth disease is a naturally occurring disease that affects hoofed animals including domesticated economic livestock such as cattle, swine, and sheep as well as wildlife such as deer. The disease is rarely fatal to the infected animal but can destroy the economic productivity of a herd and because of the highly infectious nature of HMD, it can rapidly spread throughout an entire region by infected animals, non-infected carriers such as humans, by air transmission and within various animal species. The recent outbreak of HMD since February of 2001 in Britain has shown the economic dangers of a widespread epidemic including direct economic damage in the destruction of livestock herds as well as ancillary economic damage in other areas such as a reduction in tourism through travel restrictions and security to prevent the disease from spreading from region to region or from country to country.

An Associated Press report (10-31-01 Columbia Tribune) quoted the British Tourism Minister Kim Howells with an estimate of \$4.8 Billion loss to the English tourism industry with a direct destruction of nearly 4 million British livestock. In the case of HMD disease, vaccination of herds is not usually performed due to the difficulty in differentiating between an infected animal and a vaccinated animal. Vaccinated animals are banned from export sales which is a significant consideration in most large scale livestock producers. With a HMD outbreak, quarantines and an embargo will also cause widespread economic disruption.

The U.S. has been free from HMD disease since 1929 but the economic dangers of an outbreak could be catastrophic to the pork and beef industries. An outbreak would potentially be even more difficult to eradicate than in previous U.S. outbreaks due to the proliferation of deer wildlife that has exploded in recent years due to significant conservation efforts. A resident endemic infectious population in wild deer would be disastrous to the domesticated herds, and livestock breeding or large-scale confinement production areas.

Would a potential terrorist consider HMD? Domestic eco-terrorists with an animal rights or anti-meat agenda as well as foreign enemies would consider the livestock industry a prime target for economic disruption. In April of 2001, People for the Ethical Treatment of Animals (PETA) cofounder Ingrid Newkirk expressed hope that HMD which devastated the British cattle industry would come to the U.S., "It will bring economic harm only for those who profit from giving people heart attacks" (Richard Berman, USA Today, Nov. 1, 2001).

Vaccines can keep animals from acquiring diseases, but in most cases they do not keep animals from being carriers. A cow vaccinated against HMD can carry the disease in her throat tissues for two and a half years after exposure. Also, a vaccinated animal cannot be distinguished from an infected one; the titers are the same" [2]. An even more sobering thought is the spread of the HMD into the wildlife population, such as deer, where population numbers have skyrocketed in recent years. An effort to eradicate the disease epidemic in both the commercial livestock bases of pigs, cattle and sheep as well as the deer population could reach monstrous levels. This is why the genetic efforts in vaccine production and vaccine quality is so exciting. Incorporating a vaccine into both a feed plant for animal food-stock and into forage crops for the wildlife would be critical.

In addition, it would be beneficial to have a vaccine available where the titers for infected and vaccinated animals could be easily distinguished. Sub-unit vaccines such as viral coat protein put into forage crops have the potential to accomplish that goal. "Easy, inexpensive methods of vaccination are crucial to the prevention of animal diseases in rural regions of the world" [54].

The economic considerations of HMD was demonstrated in March 21, 2001 when in North Carolina, inspectors found lesions on a dead hog at a packing plant. "Hog company stock prices fell and touched off panic selling on the Chicago Board of Trade. Tests ultimately proved it was a false alarm" (Associated Press release, Columbia Daily Tribune 12-31-01).

REFERENCES

1. TW Frazier, DC Richardson. Editors. Food and Agricultural Security. New York Academy of Sciences 894, 1999.
2. A Kohnen. Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture, BCSIA Discussion Paper 2000-29, ESDP Discussion Paper ESDP-2000-04. John F. Kennedy School of Government. Harvard University. October, 2000.
3. Bovine Alliance on Management and Nutrition (BAMN). An Introduction to Infectious Disease Control on Farms (Biosecurity), BAMN Publications, 2001.
4. CC Combs. Terrorism in the Twenty-First Century. 2nd ed. New Jersey: Prentice Hall, 2000.
5. F Hacker. Crusaders, Criminals, Crazies: Terror and Terrorism in Our Time. New York: W. W. Norton & Company, 1976.
6. GN Agrios. Plant Pathology, 3rd ed. Burlington: Academic Press, 1988.

7. DB Schweikhardt. An Assessment of the Economic Impacts of the September 11 Terrorist Attacks: Ten Tentative Conclusions, Staff Paper No. 01-41, Department of Agricultural Economics, Michigan State University, October 2001.
8. S Plous. *The Psychology of Judgement and Decision Making*, New York: McGraw-Hill, 1993.
9. HW Lewis. *Technological Risk*. New York: W.W. Norton and Company, 1990.
10. NATO (North Atlantic Treaty Organization). *Handbook on the Medical Aspects of NBC Defensive Operations, AmedP-6(B), Part II- Biological, FM 8-9*. Departments of the Army, the Navy, and the Air Force. February, 1996.
11. JL Witherly, GP Perry, Leja, L Darryl, *An A to Z of DNA Science*. New York: Cold Spring Harbor Laboratory Press, 2001.
12. AD Baxevanis, BF Ouellette, BF Francis. Editors. *Bioinformatics: A Practical Guide to the Analysis of Genes and Proteins*. 2nd ed. New York: John Wiley & Sons, 2001.
13. *Introduction to ArcGIS I. GIS Education Solutions (Course Training Set)*. ESRI Educational Services, Redlands, California, 2001.
14. MS Meade, RJ Earickson. *Medical Geography*. 2nd ed. New York: Guilford Publication, 2000.
15. JB Campbell. *Introduction to Remote Sensing*. 2nd ed. New York: Guilford Publication, 1996.
16. JR Jensen. *Introductory Digital Image Processing: A Remote Sensing Perspective*. 2nd ed. New Jersey: Prentice Hall, 1996.
17. GS Campbell, JM Norman. *Environmental Biophysics*. Heidelberg: Springer-Verlag, 1998.
18. RH Shumway, DS Stoffer. *Time Series Analysis and Its Applications*. New York: Springer, 2000.
19. PA Rogerson. *Statistical Methods for Geography*. Thousand Oaks: Sage Publications, 2001.
20. Y Pannatier. *Variowin: Software for Spatial Data Analysis in 2D*. New York: Springer, 1996.
21. AS Fotheringham, C Brunsdon, M Charlton. *Quantitative Geography: Perspectives on Spatial Data Analysis*, Thousand Oaks: Sage Publications, 2000.
22. RA Kempton, PN Fox. Editors. *Statistical Methods for Plant Variety Evaluation*. London: Chapman and Hall, 1997.

23. National Plant Board. Safeguarding American Plant Resources: A Stakeholder Review of the APHIS-PPQ Safeguarding System. USDA-APHIS-PPQ. July 1, 1999.
 24. EJ Henley, H Kumamoto. Reliability Engineering and Risk Assessment. New Jersey: Prentice Hall, 1981.
 25. NJ McCormick. Reliability and Risk Analysis. Burlington: Academic Press, 1981.
 26. SE Jorgensen. Editor. A Systems Approach to the Environmental Analysis of Pollution Minimization. Boca Raton: Lewis Publishers, 2000.
 27. TB Borak. Editor. Applications of Probability and Statistics in Health Physics. Health Physics Society, 2000.
 28. SP Millard, NK Neerchal. Environmental Statistics with S-PLUS. Boca Raton: CRC Press, 2001.
 29. PS Levy, S Lemeshow. Sampling of Populations: Methods and Applications. 3rd ed. New York: John Wiley & Sons, 1999.
 30. GM Pierzynski, JT Sims, GF Vance. Soils and Environmental Quality. 2nd ed. Boca Raton: CRC Press, 2000.
 31. MMR Williams, SK Loyalka. Aerosol Science: Theory and Practice. Oxford: Pergamon Press, 1991.
 32. LL Sanders. A Manual of Field Hydrogeology. New jersey: Prentice-Hall, 1998.
 33. M Eisenbud, T Gesell. Environmental Radioactivity. 4th ed., Burlington: Academic Press, 1997.
 34. J Neter, MH Kutner, CJ Nachtsheim, W Wasserman. Applied Linear Statistical Models. 4th ed. New York: WCB/McGraw-Hill, 1996.
 35. GC Reinsel. Elements of Multivariate Time Series Analysis. 2nd ed. New York: Springer, 1997.
 36. M Fujita, P Krugman, A Venables. The Spatial Economy. The MIT Press, 2000.
 37. F Hayashi. Econometrics. Princeton University Press, 2000.
 38. E Waltz, J Llinas. Multisensor Data Fusion, Norwood: Artech House, 1990.
 39. R Shiavi. Introduction to Applied Statistical Signal Analysis. 2nd ed. Burlington: Academic Press, 1999.
 40. ES Lander, MS Waterman. Editors. Calculating the Secrets of Life. Washington D. C: National Research Council, National Academy Press, 1995.
-

41. HM Deitel, PJ Deitel, TR Nieto, DC McPhie. Perl: How to Program. New Jersey: Prentice Hall, 2001.
42. M Watson. Programming in Scheme. New York: Springer, 1996.
43. J Han, M Kamber. Data Mining: Concepts and Techniques. Burlington: Academic Press, 2001.
44. KP Yoon, C-L Hwang. Multiple Attribute Decision Making, Thousand Oaks: SAGE Publications, 1995.
45. K Lange. Mathematical and Statistical Methods for Genetic Analysis. New York: Springer, 1997.
46. S Kaufmann. A Crash Course in Mathematica. Basel, Switzerland: Birkhauser Verlag, 1991.
47. PT Tam. A Physicist's Guide to Mathematica. Burlington: Academic Press, 1997.
48. R Maeder. The Mathematica Programmer, Chestnut Hill: AP Professional, 1994.
49. WN Venables BD Ripley. Modern Applied Statistics with S-PLUS. 3rd ed. New York: Springer, 1999.
50. A Krause, M Olson. The Basics of S and S-PLUS. 2nd ed. New York: Springer, 2000.
51. JM Poehlman, DA Sleper. Breeding Field Crops. 4th ed. Iowa State University Press, 1995.
52. OH Frankel, AHD Brown. The Conservation of Plant Biodiversity. Cambridge: Cambridge University Press, 1995.
53. D Briggs, SM Walter. Plant Variation and Evolution. 3rd ed. Cambridge: Cambridge University Press, 1997.
54. DJ Bourgaize, R Thomas, RG Buiser. Biotechnology. Boston: Addison-Wesley, 2000.

BIBLIOGRAPHY

- DL Streiner, GR Norman. PDQ Epidemiology. 2nd ed. Philadelphia: B. C. Decker Inc., 1998.
- RM Bourdon. Understanding Animal Breeding. 2nd ed., New Jersey: Prentice Hall, 2000.
- DC Coleman, DA Crossley. Fundamentals of Soil Ecology. Burlington: Academic Press, 1996.
- PJ Kramer, JS Boyer. Water Relations of Plants and Soils. Burlington: Academic Press, 1995.

PJ Fellows. Food Processing Technology: Principles and Practice. Crystal City, Virginia: Ellis Horwood Limited, 1988.

JW Polderman, JC Willems. Introduction to Mathematical Systems Theory. New York: Springer, 1998.

N Gershenfeld. The Physics of Information Technology. Cambridge: Cambridge University Press, 2000.

JC Frauenthal. Mathematical Modeling in Epidemiology. Heidelberg: Springer-Verlag, 1980.

9

Sensors and Detection Systems for Biological Agents

Tushar K. Ghosh and Mark A. Prelas
University of Missouri, Columbia, Missouri

INTRODUCTION

Detection of biological agents used for bio-terrorism is a challenging task, particularly from the outdoor environment. The shortcomings of the biological agent detection systems became rather obvious during the Persian Gulf War of 1991. A number of pathogens could not be detected immediately because of the limitation and capability of the technology that was available at that time. During the Gulf War 17 research and development systems were deployed to the Gulf region to monitor the air for suspected Iraqi biological warfare agents. Twelve of the 17 systems were mobile and the remaining five systems were static employed at critical logistic facilities. The mobile systems consisted of high volume air samplers and Sensitive Membrane Antigen Rapid Test (SMART) identification tickets. The static systems had a commercial aerosol sampler with SMART tickets. The mobile units were mounted on HUMVEES and on Isuzu Troopers equipped with high volume XM-2 air samplers. The XM-2 air samplers had low reliability and an unacceptable false alarm rate [1]. Most of these detection systems can be used for domestic applications because of the similarities in the agents that can be employed both in warfare and in terrorism. Although there are similarities in the detection systems for the battlefield and domestic counter terrorism, the needs of domestic counter terrorism differ in several major respects from their battlefield counterpart.

1. Domestic detection systems must deal with a much broader range of agents.

2. The false positive requirements are much more demanding for domestic protection.
3. Detecting an attack in the vast urban population will be extremely difficult.
4. There is much less supporting infrastructure in civilian populations.
5. The detection system must meet the needs of local law enforcement personnel, fire fighters, public health officials, and others who would likely be first on the scene following a biological attack.

Identification of biological organisms within minutes and at the parts per billion to parts per trillion concentrations level is a challenging task. A number of detection systems have been developed since the Persian Gulf war by taking advantage of the advancement in genomics, biotechnology, microengineering, and microcomputers. Although the detection systems for biological agents can be broadly classified as (a) detection of biological agents in clinical samples, and (b) detection of biological agents in the environment, the difference between the two systems is mainly in the collection of samples. Once a sample is collected (whether from patients or environment), the same methodologies and equipment can be used for specific detection and identification of the biological agents.

DETECTION OF BIOLOGICAL AGENTS IN THE ENVIRONMENT

Real-time detection and measurement of biological agents in the environment is daunting. A myriad of microorganisms are present in the environment and each organism has its own signature. Also the number of biological agents that could be employed in a terrorist attack are much larger compared to the number for biological warfare. Most detection schemes are specific for a particular biological agent. As a result civilian agencies generally do not have the capability at any level currently to detect a broad range of biological agents. A number of military units, most notably the Army's Technical Escort Unit, the U.S. Marine Corps Chemical Biological Incident Response Force, and the Army Chemical Corps, presently have some first-generation technology available.

Detection technologies are categorized by their requirement to come in direct physical contact with the biological agent. Depending on the need, the detection system architecture and sensors involved will be different. For early warning of a biological event, a "stand-off" detection system may be sufficient. However, in order to take counter measures, diagnostic capability would require "point" detection. For early warning, sensitivity of the detection system is not important. The presence of live biological agents needs to be determined. Specificity of the biological agents is not important. This is also true for the control of contaminated environments, determination of decontamination efficacy, and threat assessment. Generally the concentration level has to be far in excess of the infectious dose limit in order to infect or kill someone. Determination of dose level will require specific identification of the biological agents and a point detection system would

be required. Also, for clean-up and reoccupation of contaminated areas point detectors will be useful.

Stand-off Detection

In a stand-off detection system, detection is accomplished from a distance and does not require direct physical contact. Threat scenarios involving releases of biological agents as a line source upwind from the target are likely to happen in the battlefield; however a similar tactic may be used in domestic terrorism. Most of the agents for domestic terrorism can be delivered as aerosols. Therefore, stand-off monitors may be aimed at detecting particles of biological nature in distant clouds. Generally the size range of the biological particles is from 0.5 to 5 microns. Stand-off systems can be either active or passive. In active mode, a laser beam is focused on the target and the return energy is continuously analyzed for signature of biological agent. In a passive mode an infrared sensor is used to track, detect and collect data from particles of biological origin by analyzing their emitted energy.

Stand-off detection offers safe, real-time determination of particulates or aerosols in the atmosphere by utilizing lasers, infrared and Raman spectroscopy, and fluorescence [2]. The application of these devices is somewhat limited by their range, which is typically several kilometers. This can limit their use for urban bioterrorism scenarios. However, these devices may be used for monitoring predetermined, high-risk sites or large public gathering places, such as stadiums, for aerosol clouds. The stand-off detection is generally based on Light Detection And Ranging (LIDAR) system. A LIDAR system can be operated either in passive or in active mode.

In the passive mode the back scattering of laser light is utilized to determine the size and spatial distribution of airborne particles. The technique cannot distinguish biological particles from non-biological particles. It determines the particle size distribution in the cloud and the abrupt increase of particles in the range from 1 to 5 microns in diameter is monitored. The Los Alamos National Laboratory developed a LIDAR detection system using a 1.55 micron wavelength optically pumped oscillator laser that operates at 100 Hz, with 0.5 joules per pulse [3]. It utilizes an InGaAs detector with an 86% optical efficiency, a telescope of 75 cm in diameter, and a field view of 150 microradians. The complete unit is mounted on a helicopter and is capable of aerosol tracking and mapping at distances up to 50 km. A typical long-range LIDAR system is shown in Figure 9.1.

When operating a LIDAR system in active mode, the thermal emissions from a given direction are monitored. Fibertek Inc. [4] has developed a short range biological standoff detection system for military use that can be used in active mode. The infrared unit can provide cloud detection, acquisition and tracking capability, while the UV unit provides real time detection and discrimination between biological and non-biological aerosols using ultraviolet laser-induced fluorescence (LIF). The presence of tryptophan is detected. Since all living organisms

have tryptophan, identification of specific organisms because of the similarity of their emission spectra is not possible.

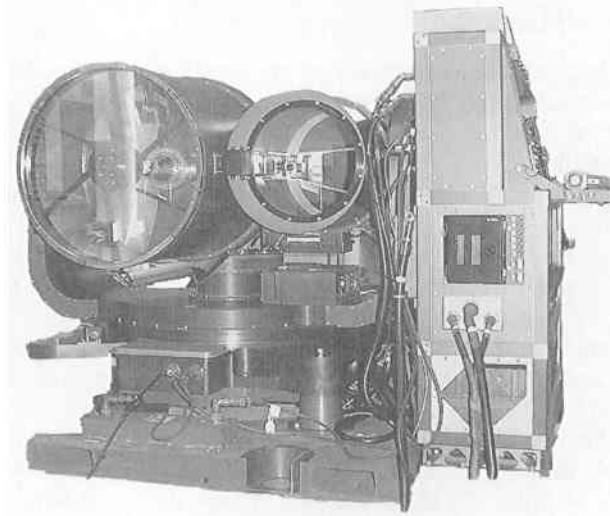


Figure 9.1 A long-range LIDAR system. Source: Military Analysis Network. <http://www.fas.org/man/dod-101/sys/land/lr-bsds.htm> [5].

The Naval Research Laboratory and Research International [6] have developed a small model airplane-like unmanned aerial vehicle (UAV) for stand-off detection. The size of UAVs can range from a few inches to a foot and carry sensors on-board capable of downloading data to a ground-based control system. Prototype vehicles have been successfully demonstrated in cities and inside buildings as well as in outdoor terrains. Furthermore, they are reusable and easily transported. In the event of biological agents being released in a building, such vehicles could locate "hot zones" and monitor decontamination efficacy, reducing human exposure and risk. Later the Naval Research Laboratory developed a remote biosensor using a fiber-optic-based sensor [7]. The complete unit that contained an automated fluidics unit for immunoassays, a cyclone sampler, a radio transceiver, and batteries weighed about 4.5 kg and was loaded on a remotely piloted airplane. This remote biosensor was able to collect bioaerosols in flight, identify them, and transmit back to the ground operator.

Prasad and his co-workers [8] have designed a new eye-safe portable digital lidar (PDL) for detection of biological agents. The detection system consisted of an 8 in. telescope, $<10 \mu\text{J/pulse}$ energy at 2.5 kHz, photon counting digital detection and 2 seconds averaging. Two tests were carried out at Dugway Proving Grounds. The portable lidar system was able to differentiate between natural and unusual clouds, and to track the aerosol cloud location, their wind speed and direction.

POINT DETECTION

Point detection refers to testing a sample that has been taken directly from the environment suspected of contamination by biological agents. This may include monitoring of the air/water systems in buildings for general pathogen contamination or contamination by specific biological agents. Although the objective of point detection is to specifically identify and quantify the targeted biological agent, in many situations neither exceptional sensitivity nor exceptional specificity is required. Assessment of the total microbial content may be sufficient to determine contamination and alert personnel to danger. A sharp and unexplainable rise in total microbial count probably should be sufficient to trigger protective action, regardless of whether the specific pathogen can be identified. More precise identification would be important for forensic uses, and for optimal treatment of many agents (e.g., broad-spectrum antibiotics might be prescribed as soon as the agent is identified as bacterial, even if the species is unknown). Depending on the specific needs, a point detection system may contain various components.

1. Sampling devices.
2. Non-specific detection systems.
3. Specific detection systems.

Sampling Devices

Air sampling of microorganisms is governed by the same principles of collection as other particulates; however, the viability of organisms complicate their collection. The main objective here is to keep the collected microorganisms in a viable state so that subsequent identification steps become easier. Because of this requirement, special handling and processing techniques are necessary since analytical identification and enumeration of collected organisms are different from other non-biological particulates. Several points need to be considered in selection of a sampler for biological agents [9].

- 1) A single sampler may not be effective for all types of agents.
- 2) No sampling device provides 100% recovery of bioaerosols.
- 3) Viability of bioaerosol samples must be maintained in the sampler for subsequent growth and identification.
- 4) The efficiency of the sampling device depends on the size of a particular organism.
- 5) The survival and growth of individual organisms depend on the temperature, pH, and nutritional content of the collection media.
- 6) Samplers must be operated and used according to the manufacturer's specifications.

Most instruments used for identification of biological agents require a liquid sample. As a result, airborne microbes are extracted from aerosols or particulates in a liquid. This not only is a very efficient method of extracting the microbes but at the same time they can be in a concentrated form for direct use in subsequent equipment. Four general types of sampling devices are available to accomplish one or more of these objectives. They are: (1) viable particle-size impactors, (2) virtual impactors, (3) cyclone samplers, and (4) bubblers/impingers. Each of these technologies is described below.

Viable Particle-Size Impactors

The viable particle-size impactors usually have multiple stages connected in series or stacked one over another, which is also called a cascade impactor. Each impactor is called an impactor stage and contains a number of precision-drilled orifices. They are arranged in order of cutoff size with the largest cutoff size first. The cutoff size is reduced in each stage by decreasing the nozzle size or the number of nozzles in that stage. The most common type of impactor used for collection of bioaerosol is known as a six-stage Andersen impactor. Each stage contains 400 holes. Immediately below each stage is a petri dish containing agar or other suitable growth medium. Air is typically drawn through the impactor at a rate of 28.7 L/min. The jet velocity is uniform in each stage but increases in each succeeding stage due to a decrease in the diameter of holes in consequent stages. When the velocity imparted to the particle is sufficient, its inertia will overcome the aerodynamic drag and the particle will leave the stream of air and deposit on the agar medium. The impaction mechanism is shown in Figure 9.2. Otherwise, the particle continues to travel to subsequent stages. Each succeeding stage will remove the largest particles with the last stage collecting remaining particles. A six-stage Andersen impactor with the nozzle plate and impaction plate is shown in Figure 9.3. Although impactors can be used directly to collect bioaerosols and require no further processing of samples, they have several disadvantages, particularly if employed to collect biological agents used in a terrorist attack. The choice of nutrient has to be microorganism specific. Not necessarily all the microbes can be grown in one type of nutrients. Also, the incubation period can be anywhere from 1 to 10 days depending on the type of microbes. In the event of bioterrorism, rapid identification, preferably within hours, may be necessary.

Virtual Impactors

A virtual impactor is similar to a viable particle-size impactor, but uses a collection probe instead of a petri dish as its impaction surface. It separates particles by size into two airstreams. The impaction surface is replaced with a virtual space of stagnant or slow-moving air. Large particles are captured in a collection probe rather than impacted onto a surface. The cutoff size of the particles is controlled by controlling the ratio of major to minor flow rate. An accelerating nozzle directs the aerosols toward a collection probe resulting in a diversion of 90° away

from the collection probe. This creates a major flow path and a minor flow path. The separation of particles from the air stream takes place at this point. Small particles with low inertia follow the flow streamlines and are carried away radially with the major flow. Large particles with greater inertia deviate from the streamlines and continue moving axially in their forward path down the collection probe with the minor flow. The separation efficiency curve is determined by the ratio of the major and minor flows and the physical dimensions of the nozzle and collection probe.

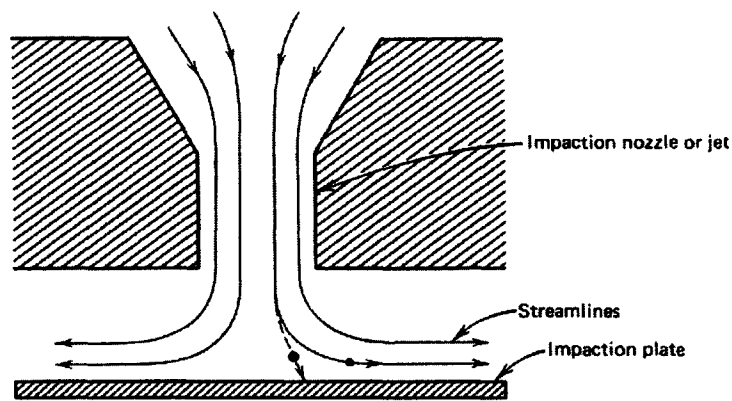


Figure 9.2 Impaction mechanism of particles in an impactor. (Source: WC Hinds, *Aerosol Technology: Properties, Behavior, and Measurement of Airborne Particles*. Printed with permission) [10].

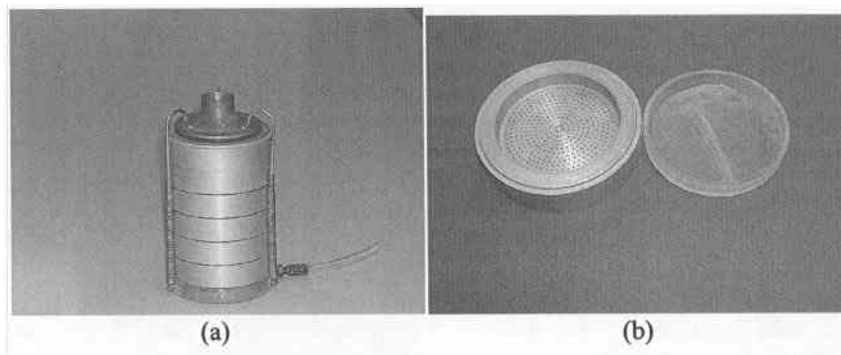


Figure 9.3 A six-stage Andersen impactor for collection of viable particles from air (a). A petri dish and an impactor with the holes are also shown in the figure (b).

Particles smaller than the cut-size of the impactor remain in both the major and minor flows. But particles larger than the cut size become concentrated in the minor flow.

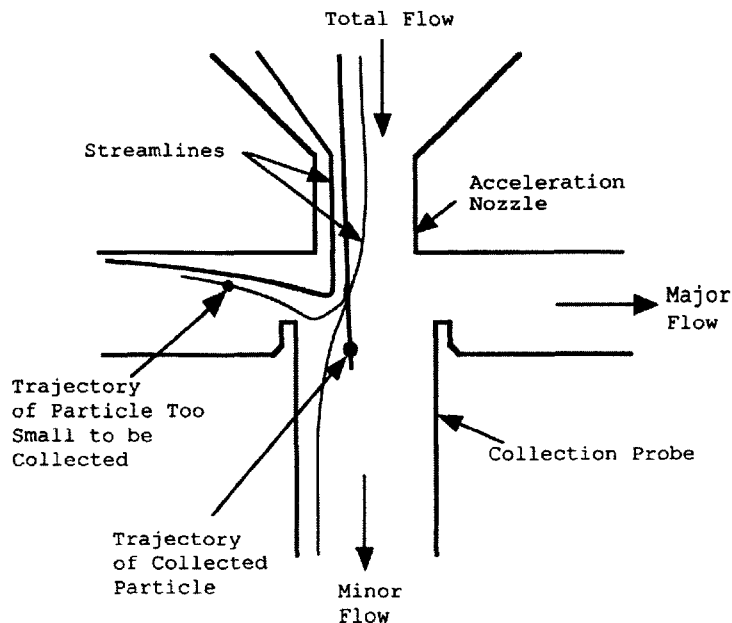


Figure 9.4 A schematic of the flow path inside a virtual impactor (with permission from TSI Inc., St. Paul, MN, USA).

Several virtual impactors can be stacked one over another. In this way the particles can be concentrated to many times the original concentration before collection. The final stage can then impact the particle stream into a liquid, resulting in a highly concentrated liquid sample. In Figure 9.5 is shown a schematic of a two stage virtual impactor. Three collection filters and two virtual impactors are assembled in a compact concentric unit with cylindrical symmetry. The total flow is controlled with a personal air sampling pump and the split at each stage is controlled by a flow orifice.

Virtual impactors can be used to collect and concentrate the particles for direct feeding to other units such as Chemical Biological Mass Spectrometer (CBMS). Griest et al. [11] collected bioaerosols by an opposed jet virtual impactor for analysis by their CBMS unit. Several modifications to the original design of a virtual impactor have been proposed by various researchers to improve its performance. Gotoh and Masuda [12] have developed an annular jet-type virtual impactor. The new impactor had a better performance compared to the impactor with

a rectangular jet because the annular jet has no end, which causes the deterioration of the performance in the rectangular jet-type impactor. To increase the sampling flow of the virtual impactor, Ding et al. [13] developed both multinozzle and longer slit configurations. According to them, a longer slit nozzle increased the inlet flow more effectively than using multiple nozzles.

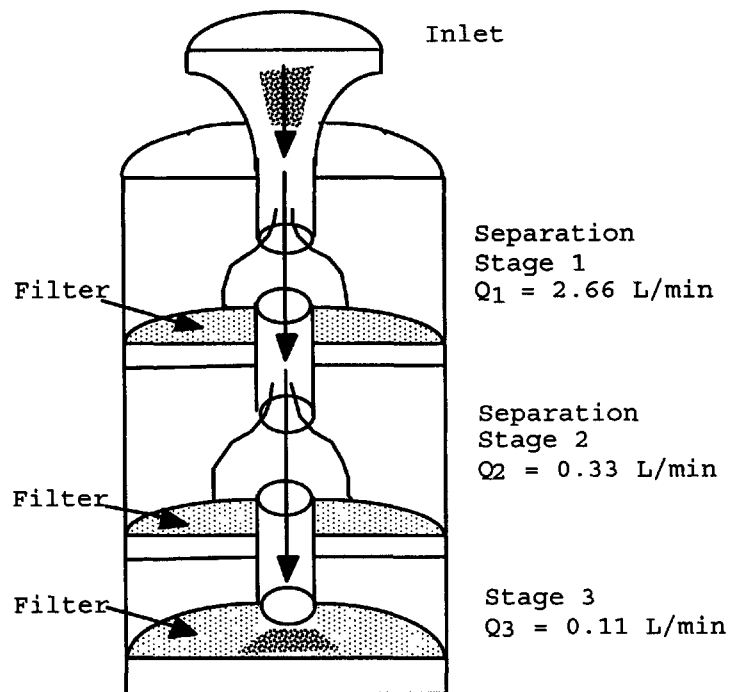


Figure 9.5 Schematic of a 2-stage virtual impactor. (With permission from TSI Inc., St. Paul, MN, USA.)

Cyclone Sampler

In a cyclone sampler, a particle-laden air stream is introduced tangentially near the top of a cylinder. The air stream flows spirally down the chamber following the inner wall, then reverses towards the end and spirals up the center of the chamber and out through the exit. Larger particles are collected on the outer wall due to centrifugal force. Smaller particles follow the airstream that forms the inner spiral and leave the cyclone through the exit tube. The working principle of a cyclone sampler is shown in Figure 9.6. Application of a water spray to the outer walls of a cyclone facilitates particle collection and preservation. Also a pump may be used to inject liquid into the air inlet to wash particles deposited in the

inner walls of the chamber into the collection vessel at the bottom. Sometimes a detergent is added to ensure proper wetting of the wall. Air sampling rate can be varied from 75 to 1000 L/min depending on the size of the cyclone. A cyclone sampler is shown in Figure 9.7.

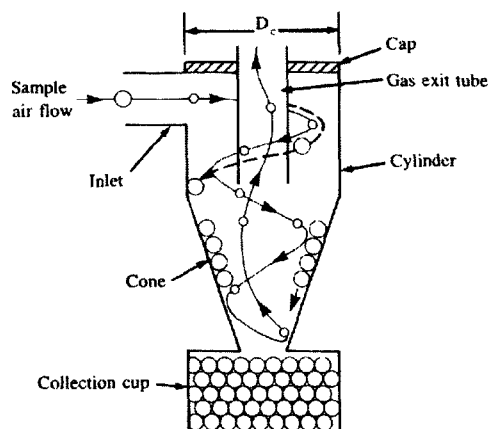


Figure 9.6 Particle collection mechanism in a cyclone sampler. (Source: Bioaerosol Handbook. Eds. Cox and Wathes. CRC Press) [14].

The samples collected by cyclone samplers can also be in concentrated form and can be fed directly to an instrument for identification. Ligler et al. [15] used a cyclone type air sampler while testing a remote sensing unit for analysis of biological agents. The cyclone sampler was able to collect aerosolized bacteria in flight. Griffiths and Stewart [16] compared the performance of five industrially important bioaerosol samplers with that of a glass wet-walled and a cyclone sampler. The test aerosols were *Saccharomyces cerevisiae* and *Penicillium expansum* spores. The cyclone sampler and Andersen microbial sampler met the basic criteria for a suitable sampler for airborne bioaerosols.

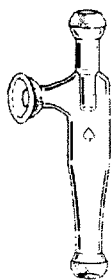


Figure 9.7 A cyclone sampler from Ace Glass Inc., Vineland, New Jersey.

Bubblers/Impingers

In this type of sampler, usually an air jet is impinged into the liquid contained in the sampler. As the air passes through the liquid, the aerosol particles are captured by the liquid surface at the base of the jet. In order to collect the smallest particles possible, the jet is typically made with a small critical orifice causing the flow to become sonic. The most common type of impinger is called all-glass impinger or AGI-30 (Figure 9.8). The jet is raised to 30 mm above the base of the sampler to minimize the impact of the viable microorganisms with the base of the sampler and therefore to increase the capture efficiency of viable particles.

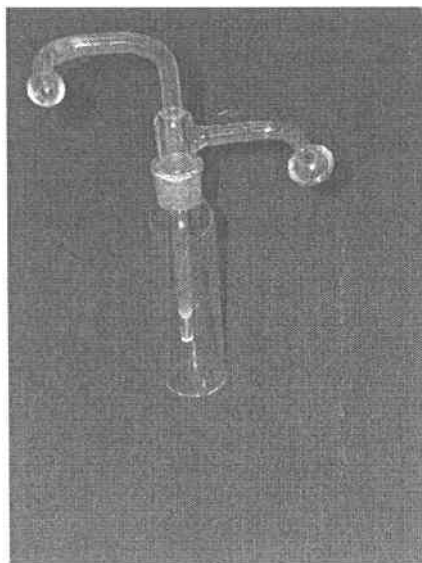


Figure 9.8 An all glass impinger for collection of airborne microbes.

Although any of these samplers can be used to collect samples from the atmosphere, prior knowledge of the characteristics of the microorganisms are important to devise a collection strategy or to choose a correct sampler. The environment in which the target microbe exists can significantly affect the physiology of the microbe and their detection procedure. For example, *Bacillus anthracis* that causes anthrax exists as a hard, oval, inactive spore in the atmosphere and is highly resistant to sunlight, heat, and disinfectants. However, in tissue, including blood, it germinates into a rod-shaped vegetative bacillus actively proliferating and producing its characteristic toxins. Therefore, the detection of *Bacillus anthracis* from air will be different than in the blood. Also, the growth state and gene expression of the collected agents may depend on the growth or collection media. Another issue that should be kept in mind is the very low concentration of these airborne microbes in the environment. Therefore if a proper sampler is not se-

lected, enough microbes may not be collected by the sampling unit leading to false negative in subsequent analysis.

Non-Specific Detection

Non-specific detection is generally used as a “trigger” to monitor for the presence of biological agents. Generally a sudden increase in the atmospheric particulates in the size range of 1 to 5 μm above the background level is monitored. Both the biological and non-biological particles are counted. However, a more sophisticated detection system can differentiate between biological and non-biological particles.

Aerodynamic Particle Sizing

Aerodynamic Particle Sizing (APS) can be used as a simple trigger for the presence of biological agents and for counting the relative number of particles in specific size ranges. A schematic diagram of an APS system is shown in Figure 9.9. The particle laden air stream, drawn into the system through a flow nozzle, produces a controlled high-speed aerosol jet. The air velocity at any point in the flow field stays constant during the measurement period. However, individual particles accelerate at different rates within the jet, based on the size of the particles. Smaller particles accelerate at a higher rate than the larger particles since particle velocity at any given point is inversely proportional to the aerodynamic size of the particle. A laser beam measures the time-of-flight of the individual particles. The beam is split into two parallel beams, and as the particles pass through them, a pair of electrical pulses are produced by forward-scattered light, collected and sensed with a photomultiplier tube. A high-speed clock measures the time between the electrical pulses (time-of-flight). The aerodynamic particle size is calculated with a previously stored calibration curve. Particles are thus counted and sized for a specified sampling period, and results displayed as a histogram of aerodynamic diameter versus number.

Fluorescent Aerodynamic Particle Sizer (FLAPS)

The Fluorescent Aerodynamic Particle Sizer is the modified version of the APS system. An additional laser (blue or ultraviolet) is employed to detect aerosol particle fluorescence in addition to aerodynamic particle size. The second laser beam is located downstream and is perpendicular to the standard dual laser beams. FLAPS examine a concentrated aerosol sample for biological fluorescence and compare this response to background particle size characteristics. Thus FLAPS can discriminate between non-biological and biological aerosols. A FLAPS functions on the principle of flow cytometry technique. The particle size and fluorescence for each particle in an air stream are measured. This permits it to distinguish between biological aerosol particles and non-biological material like sand. A HeNe laser provides the size measurements of the respirable particles (0.5-15 μm size range) by the time-of-flight method. Molecular excitation of biological parti-

cles for fluorescence measurement is initiated by HeCd UV laser at 325 nm. Particles containing molecules that are excitable at this wavelength emit light at between 400-580 nm. Fluorescence characteristic is suggestive of biological properties inherent with the particle.

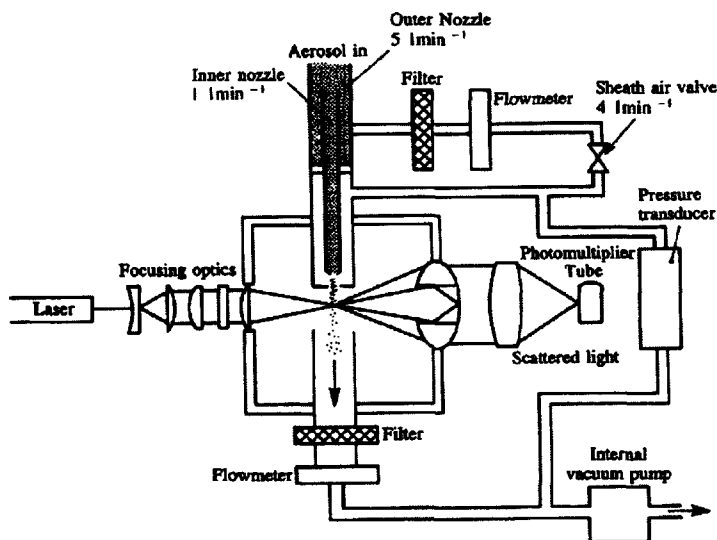


Figure 9.9 Schematic diagram of APS flow system (With permission from TSI Inc., St. Paul, MN, USA).

Recent efforts include employment of UV laser-induced fluorescence (UV LIF) for diagnostic measurement of biological agents. Most of these techniques utilize quadrupled Nd:YAG laser at 266 nm in the ubiquitous tryptophan absorption band from 260-290 nm [17-22]. However, a number of researchers have employed UV wavelength at 355 nm [23-26]. The FLAPS developed by Ho et al. [27] measures fluorescence signals of single spores under flow cytometry using UV excitation at 340-360 nm. They later developed a second generation FLAPS (FLAPS2) that was smaller, power efficient and field portable. Field testing of FLAPS2 with spores of *Bacillus subtilis var niger* showed that FLAPS technology can measure fluorescence signals from single particles in an aerosol. Eversole et al. [28] at Naval Research Laboratory developed a prototype Single Particle Fluorescent Analyzer (SPFA) and compared its performance against a FLAPS in outdoor settings. The SPFA system differentiated between biological and non-biological particles using particle size and intrinsic UV fluorescence excited by 266 nm laser pulses. It detected at least 87% of the released particles. Individual particle data were also obtained in the visible fluorescence band that could be used for some identification.

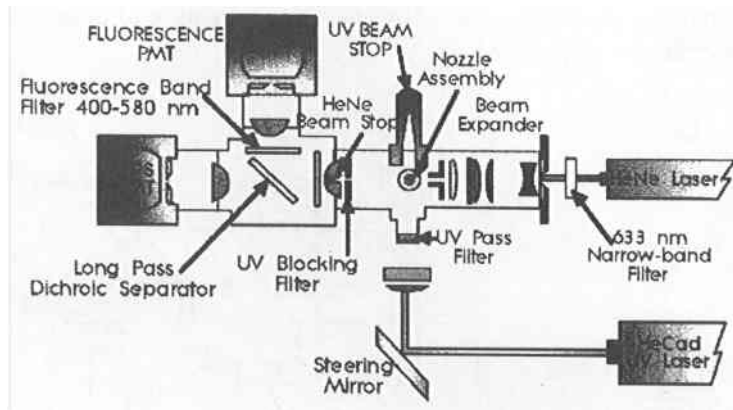


Figure 9.10 A schematic diagram of FLAPS system (With permission from TSI Inc., St. Paul, MN, USA).

Flow Cytometry

Flow cytometry is used to measure certain physical and chemical characteristics of cells or particles as they travel in suspension one by one in a fluid stream through a light source. The current flow cytometer consists of a laser, collection optics, electronics and a computer to translate signals to data. Scattered and emitted fluorescence are measured. A fluorescent dye may be added to cells to measure other characteristics. Since the measurements are made on individual cells, detection of specific organisms in a complex mixture of other biological and non-biological particles is possible. The modern instruments can make measurements at rates of up to 10,000 particles/second.

In flow cytometry cells must be sorted physically into a single cell or particle of interest from a heterogeneous population. Cells are aspirated from a sample and ejected one by one from a nozzle in a stream of sheath fluid which can be any ionized fluid. The cells are then electrically charged and electrostatically deflected to the proper stream. As the cell is intercepted with the laser beam, scattered light and fluorescence signals are generated and measured using appropriate electronics. The process is shown in Figure 9.11.

A laser beam interacts with each individual cell as it passes through a flow cell constructed with optical windows as part of the coaxial arrangement. Excitation of the molecule is accomplished using an argon ion laser at 488 nm, which is close to the absorption maximum of the common fluorochrome fluorescein isothiocyanate (FITC). A more sophisticated system may incorporate a tunable laser to cover a wide range of wavelengths. Laser beams are usually focused to a

spot between 10 and 60 microns in diameter and only a few microseconds are required for a cell to travel to this spot. The optical arrangement of a typical flow cytometer is shown in Figure 9.12.

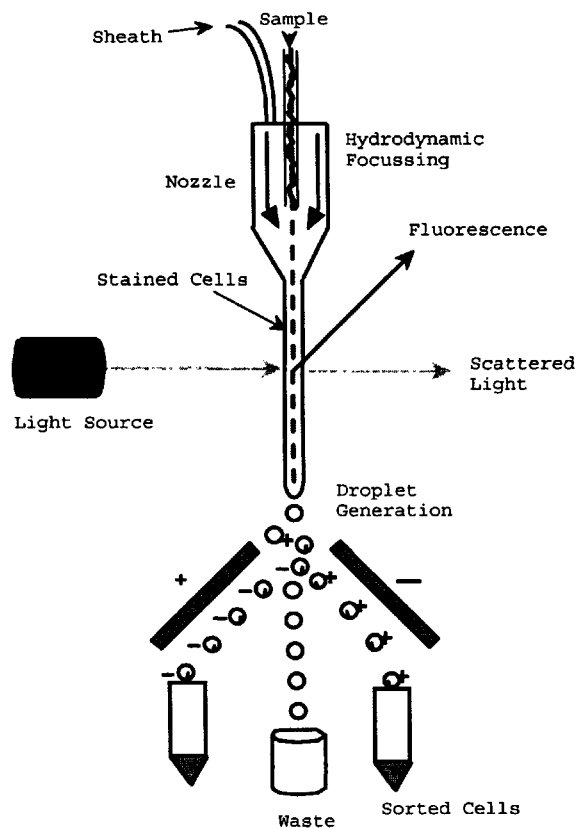


Figure 9.11 Schematic of a flowcytometry system (Source: www.flow-cytometry.de/start.html).

The flow cytometry has widespread application both in medical fields and detecting biological agents [29]. Additionally, flow cytometry technology can provide structural characteristics of biological cells (See Table 9.1). Stopa et al. [30] at US Army Edgewood Research Center worked on development of flow cytometry based biological detection systems. Their results showed that flow cytometry analyzed aerosol samples effectively, but was dependent on the dye used for staining the liquid. The samples consisted of liquid impinger fluids collected during 40 releases of 4 different simulants: *Bacillus subtilis var. niger* (BG spores), *Erwinia herbicola*, MS2 coliphage virus, and ovalbumin. When using

CPO dye the detection reliability was 50% and it increased to 70% when YOYO-1 dye was used.

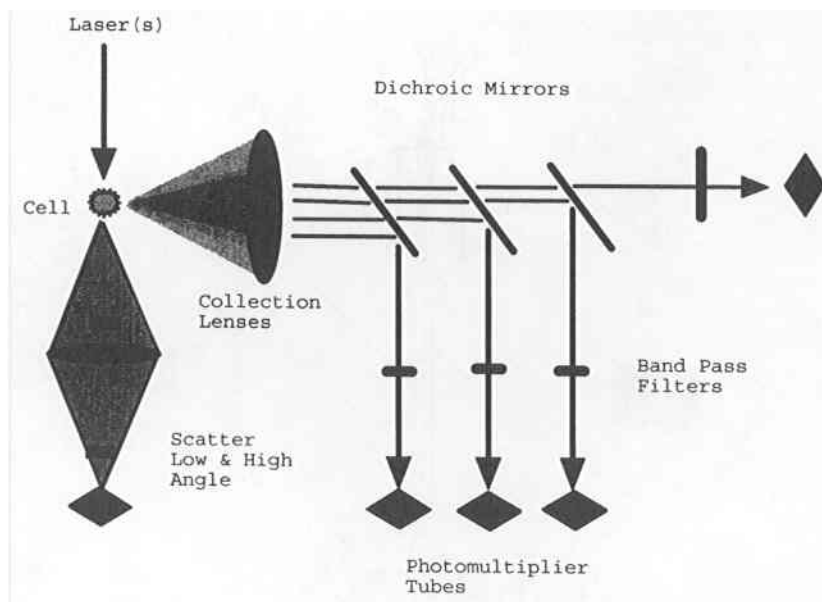


Figure 9.12 A typical optical arrangements of a flowcytometry system.
(Printed with permission. www.uwcm.ac.uk/study/medicine/haematology/cytonetuk/introduction_to_fcm/optics.htm)

Table 9.1 Structural characteristics of biological agents measurable by flow cytometry [31]

Parameter	Measuring Method
Cell size	Extinction or small angle light scattering
Cell shape	Pulse shape analysis
Cytoplasmic granularity	Large angle light scattering, electronic impedance
Birefringence	Polarized light scattering

Portable Biofluorescence

During the Gulf War, a UV-excited fluorescence technique was examined for detection of bioaerosols. The sensor developed based on this technique was called the Portable Biofluoro-Sensor (PBS). The performance was mixed during

the Gulf War, however since then, significant improvement has been made and it has become more reliable. In this method, tryptophan in BW agents was targeted for detection by the fluorescence approach. Using a photon energy in the UV region of the spectrum, tryptophan in the biomolecule is excited. The excited component spontaneously reverts to an unexcited state followed by emission of light at higher wavelengths (Figure 9.13). The emission of light depends upon the specific type of molecular component being irradiated and the excitation wavelength. This provides a unique spectrum for that particular component. This emission spectrum can be used to identify a component in a complex mixture. Since all of the biological agents have a common compound, tryptophan, the biofluorescence approach specifically targets this chemical. A typical spectrum is shown in Figure 9.14.

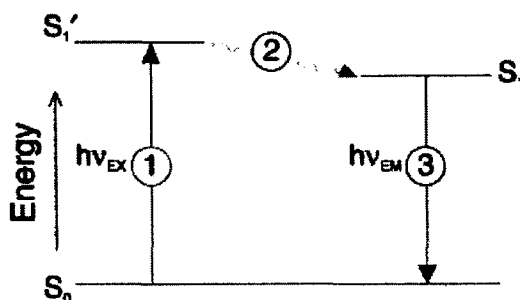


Figure 9.13 Excitation of molecules by a laser.

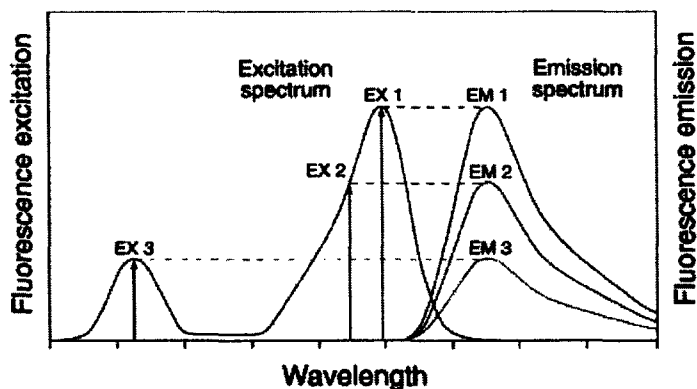


Figure 9.14 A typical emission spectrum from a biofluorescence sensor.

Biofluorescence techniques may be divided into two categories; (a) primary fluorescence, and (b) secondary fluorescence. In the primary biofluorescence method naturally fluorescent components of the biomaterials, such as tryptophan,

are used. The primary approach requires the least amount of analysis time and sample preparation. In the secondary fluorescence method, a special fluorophore (i.e., fluorochrome stain) is added to the sample before UV-irradiation. Such methods do not depend on the existence of a natural fluorophore within the targeted compound. Secondary methods, however, require a longer measurement time. Generally a filtered, pulsed xenon lamp is used in the 200 nm to 285 nm spectral region for excitation. Fluorescence usually occurs between 310 nm and 360 nm. Fluorescence spectral intensity at several wavelengths is measured with two or more filtered photomultiplier tubes or solid-state avalanche photodiodes. Although both the air and liquid samples can be used, liquid samples provide better efficiency than airborne samples.

The techniques described in this section utilize signals from fluorophores contained within particles of biological origin. Mainly tryptophan and nicotinamide adenine dinucleotide which is associated with metabolic processes are targeted for signal generation [32]. So far single-wavelength excitation and single wavelength emission fluorescence have been used for particle analysis [33]. However, the performance of biofluorescence sensors may be increased by acquiring fluorescence emission at several wavelengths [34]. Tjärnhage et al. [35] obtained spectral data from the biological warfare agent simulants at eight different excitation and emission wavelength combinations. The data were collected using a system consisting of a cyclone sampler and a commercial spectrofluorometer. Using this technique, they were able to separate biological from nonbiological particles such as dust and smoke. Also biological agents could be differentiated from each other using the measured fluorescence signals.

Specific Detection Technologies

Specific detection/identification systems are designed to identify the specific types of biological agents. Most of the methods have been designed for analysis of clinical samples. However, once a sample is collected from the environment the same instrument can be used to identify the microbes present in the sample. The specific identification systems can be broadly classified as:

- Mass spectroscopy based identification, and
- Identification by targeting at the molecular level.

Mass Spectroscopy Based Identification

Mass spectrometers (MS) characterize compounds based on their specific mass profiles, following limited fragmentation by an energy source. The mass fraction is next ionized using an ion source. MS uses the difference in mass-to-charge ratio of ionized atoms or molecules to separate them from each other. The biological agents contain lipid or fat which has a distinctive structure. This provides unique fragmentation patterns that can be used to identify biological agents. Steps involved in MS based analysis includes creation of gas-phase ions, separa-

tion of the ions in space or time based on their mass-to-charge ratio and measurement of the quantity of ions of each mass-to-charge fraction. Therefore, an MS consists of an ion source to create gas phase ions, a mass selective separator to separate the ions in space or time based on the mass-to-charge ratio and an ion detector to quantify the ions. The main challenge in MS is creation of gas phase ions. The separation of ions in space and time is rather standard nowadays. Most of the MS use the time-of-flight method for separation of charged ions. The quantification of ions by their mass-to-charge ratios is accomplished using a quadrupole mass detector.

Laser Pyrolysis

In this method, a particle beam is produced when aerosols expand through a nozzle into a vacuum and is introduced into the mass spectrometer chamber [36, 37]. Using multiple lasers, individual particles are pyrolyzed into small mass fragments and ionized by a laser pulse while in flight in the beam (Figure 9.15). A burst of ions is produced from individual particles after volatilization and ionization by electron impaction in the ion source of the mass spectrometer. The mass spectrometer detector then measures the intensities of the ions. Intensities of different mass fractions are obtained and compared with a library of mass spectral data of different microbes grown under different conditions for identification by comparison. Figure 9.16 shows mass spectra of three different bacteria.

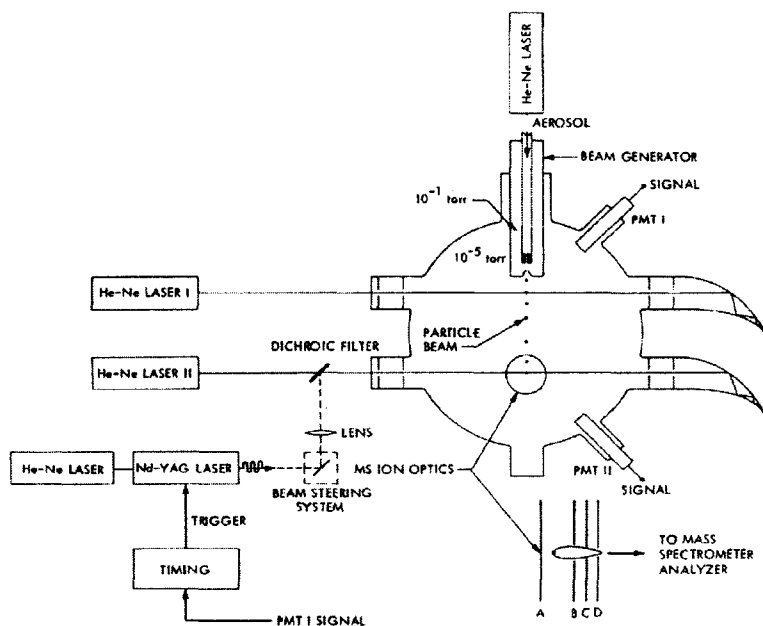


Figure 9. 15 Laser pyrolysis MS system [36].

Fast Atom Bombardment

Further improvement in microbial analysis using MS has been achieved by applying Fast Atom Bombardment Mass Spectrometry (FABMS) [38]. This method works best for polar and higher molecular weight compounds such as peptides and other biomolecules. FABMS utilizes a fast moving beam of neutral atoms targeted towards a metal coated with a liquid matrix in which the sample is dissolved. Phospholipids and other polar lipids are selectively desorbed from a lysed bacteria to provide molecular ions. There is no extraction of the lipids involved. The FABMS method can be used in positive and/or negative ion modes with a selection of matrices. Generally pseudo-molecular ions together with some fragment ions having lower mass are formed.

ElectroSpray Ionization

ElectroSpray Ionization (ESI) is one of the more recent ionization techniques that is finding rapid use in identification of microbes due to their very high sensitivity [39, 40]. In this method, a dilute solution of the analyte flows through a stainless steel capillary tube at the rate of about 1 mL/min. A high negative or positive electric potential in the range of 3 to 5 kV is applied to the end of the tube. The strong electric field at the end of the capillary pulls the solution into a Taylor cone and at the tip of the cone the solution is nebulized into small charged particles (see Figure 9.17).

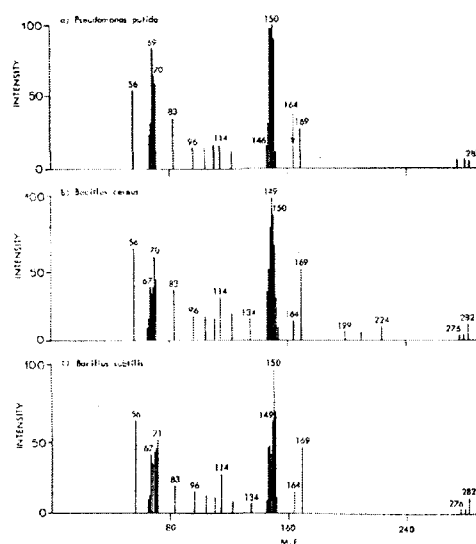


Figure 9. 16 MS spectra of several bacteria [37].

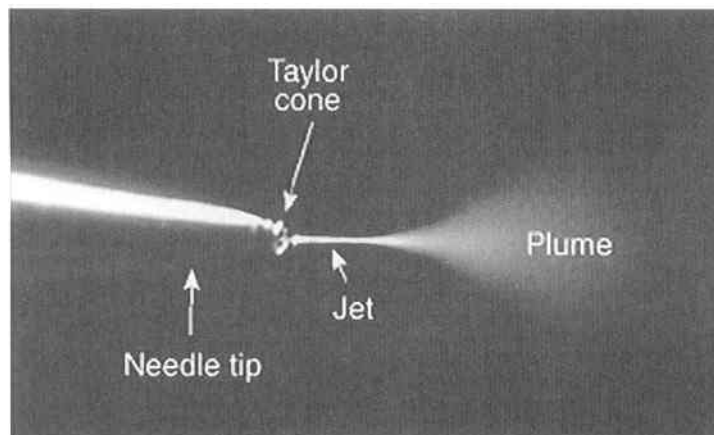


Figure 9.17 Taylor cone.

The charged droplets travel towards the counter electrode through an evaporation chamber. In this region, solvent evaporates rapidly from their surfaces and shrink in size. As the droplets get smaller, the electrical surface charge density increases causing fragmentation due to the repulsive force on the charged droplet resulting formation of a fine mist (particles). A schematic diagram of electro spray ionization system is shown in Figure 9.18.

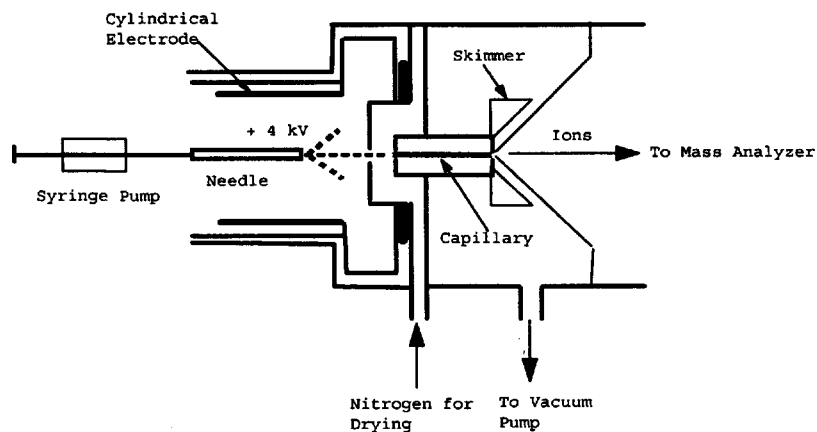


Figure 9. 18 Electro spray ionization system (Printed with permission, Paul Gates: <http://www-methods.ch.cam.ac.uk/meth/ms/theory/esi.html>).

The ions and cluster ions generated from the sample have much greater molecular mass, and, therefore, momentum than those of the solvent and move towards the target at the end of the inlet region. To assist evaporation of the droplets and the breaking up of unwanted cluster ions, a drying gas (nitrogen) flows along and past the end of the capillary. The ions then pass through two evacuated regions via a nozzle and a skimmer. These conically shaped holes refine the separation of sample ions from solvent ions on the basis of momentum; however, electrical potentials applied to the nozzle and skimmer also aid in the separation. Finally, sample ions flow into the analyzer of the mass spectrometer where their mass-to-charge ratios are measured by a quadrupole mass detector.

Matrix Assisted Laser Desorption and Ionization

Matrix Assisted Laser Desorption and Ionization (MALDI) is one of the most successful ionization methods for the mass spectrometric analysis and investigation of large molecules. This technique allows for vaporization and ionization of non-volatile biological samples from a solid-state phase directly into the gas phase. Various components of an MALDI system are shown in Figure 9.19.

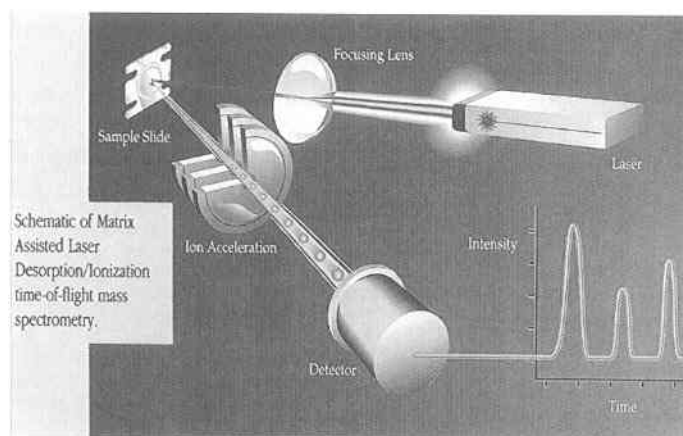


Figure 9.19 MALDI system (Thermo Electron Corporation).

The sample (analyte) is suspended or dissolved in a solid or liquid matrix which strongly absorbs laser light. Matrices are small organic compounds that are co-crystallized with the analyte. The sample is mixed with a matrix at molar ratios of 1,000:1 to 10,000:1 matrix to sample, to assist in the analysis of large, fragile molecules. It seems that the presence of the matrix, spares the analyte from degradation, resulting in the detection of intact molecules as large as 1 million Dalton mass. The matrix for biological analysis is usually a large organic compound such as 2,5-hydroxybenzoic acid, with certain properties such as high absorption at the

laser beam that prevents the decomposition of fragile samples like proteins and oligonucleotides. A detailed review on MALDI ionization mechanisms has been given by Zenobi and Knochenmuss [41].

Upon laser irradiation (usually with a pulsed laser), the matrix absorbs light resulting desorption and ionization of analyte. The ions enter the mass spectrometer, most commonly a time-of-flight mass spectrometer. A spectrum of ion intensity as a function of the travel time is recorded. A library of MALDI mass spectra has been generated for about 100 different pathogens, nonpathogens and pure known proteins [42].

Mass spectrometer based identification of biological agents is becoming a viable tool because of the recent developments that have made these systems fieldable [43]. Snyder et al. [44] used a pyrolysis-gas chromatograph ion mobility spectrometer to discriminate between aerosols of BG spores, EH and ovalbumin. The Block II Chemical Biological Mass Spectrometer (CBMS) developed by Griest et al. [11] is capable of detecting and identifying both chemical and biological agents on the battlefield.

Identification by Targeting at the Molecular Level

Biological agents can be in the form of vegetative cells and spores, viruses, and toxins. These agents can be identified by using nucleic acid or immuno-based methods. Also their products such as antigens and toxins can be targeted for identification purposes. An identification scheme will look like the one shown in Figure 9.20.

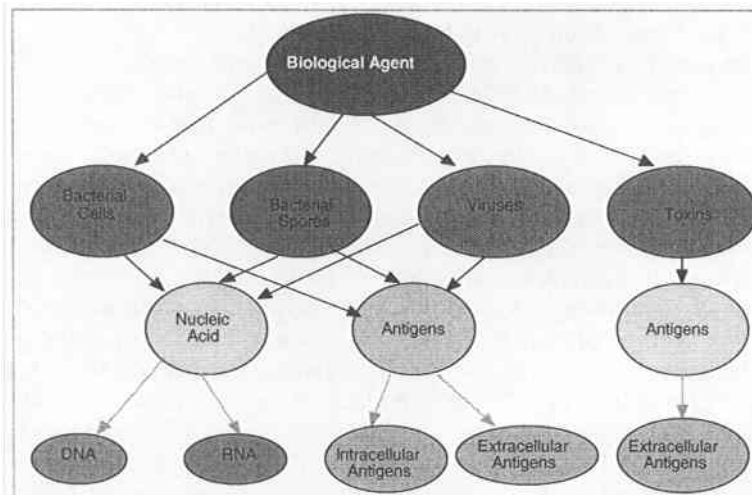


Figure 9.20 Analysis at the molecular level. (Reprinted with permission from Biosensors & Bioelectronics, 15:549-578, 2000) [45].

When identifying biological agents by targeting at a molecular level, detection system requires two components: (1) a probe, and (2) a transducer. A probe deals with how the assay or detection device recognizes the particular target microbe. The transducer technology deals with how the assay or detection device communicates the activity of the probe to the observer. The probe and transducer together determine specificity, sensitivity, and time required to make an identification. Most of the current systems incorporate both the probe and the transducer into a single unit. Probe technologies are generally based on nucleic acids, antibody-antigen binding, and ligand-receptor interactions, whereas main transducer technologies include electrochemical, piezoelectric, colorimetric, and optical systems. The transducer system acquires signals that are unique to the probe system and generate low noise signals that can be further processed without degradation to provide a signal that is related to the microbe concentration.

Nucleic Acid-Based Identification Systems

All living organisms essentially can be discriminated on the basis of nucleic acid (DNA and/or RNA) sequences unique to that particular organism. Each type of organism has some unique sections of DNA or RNA. This unique DNA structure of each organism can be used to identify pathogens and biological warfare agents. Nucleic acid-based probes capitalize on the extreme selectivity of DNA and RNA recognition. These probes and their binding can be detected directly or by tagging with an easily detected molecule that provides a signal. Therefore, nucleic acid-based detection systems can be divided into two categories: (1) direct target probing with signal amplification, and (2) target amplification.

Direct Target Probing with Signal Amplification

The basis of virtually all nucleic acid targeted probe systems is the ability of engineered single strands of RNA or DNA to bind specifically to strands of complementary nucleic acids from pathogens to form stable hybrid complexes. Most systems use sandwich hybridization involving two probes. One probe targets the nucleic acid that is captured by an oligonucleotide capture probe which is immobilized on a solid support and has sequences complementary to the target. A second oligonucleotide probe which carries a covalently attached label or reporter molecule hybridizes to a complementary region on the target for signal generation. The design of the probe can be highly specific if there is a good fit to a pathogen-unique region of the target nucleic acid, or it can provide more generic identification if there is a fit with a region of nucleic acids conserved among several related pathogens. The sensitivity of these hybridization assays for bacteria is between 1,000 and 10,000 colony-forming units. The capture target is detected by virtue of a linked reporter probe labeled with the enzyme alkaline phosphatase. A variety of reporter molecules including radioisotopes, fluorophores, enzymes, or haptens can be used. Among these reporter molecules, enzymes are most widely used which utilizes biotin-streptavidin. The probe is labeled with biotin. Streptavidin-enzyme

complex then binds to the biotinylated signal probe and detects presence of the target. The final readout is generally calorimetric.

The time-consuming part of the method is in the sample preparation and the time required to detect the signal. However, the main advantages of nucleic acid-based methods are in their universality, sensitivity and adaptability, and multiplex capabilities for a host of different microbes. Disadvantages of this technology include difficulty in isolation and "clean-up" of DNA samples, degradation of the nucleic acid probes, and interference from related sequences or products.

Target Amplification

Nucleic acid based detection has been greatly improved due to the development of amplification processes for the target organisms *in vitro*. These amplification processes are capable of generating enormous copies of target nucleic acid from a single copy. The amplification or copying of target nucleic acid is accomplished through Polymerase Chain Reaction (PCR) [46-50]. PCR involves enzymatic replication of a target region of nucleic acid defined by a set of oligonucleotide primers. A target DNA sequence can be selectively amplified or enriched to several millions in just a few hours. Within a dividing cell, DNA replication involves a series of enzyme-mediated reactions, whose end result is a faithful copy of the entire genome. A PCR reaction is carried out in the following manner [51].

- A small quantity of the target DNA is mixed with a buffered solution containing DNA polymerase, oligonucleotide primers, the four deoxynucleotide building blocks of DNA, and the cofactor $MgCl_2$.
- The mixture is heated at 94-96°C for one to several minutes during which the DNA is denatured into single strands.
- The mixture is then cooled to 50-65°C during which the primers hybridize to their complementary sequences on either side of the target sequence. This may take one to several minutes depending on the probe.
- Finally, the mixture is again heated at 72°C for one to several minutes during which the polymerase binds and extends a complementary DNA strand from each primer.

The DNA sequence between primers doubles after each cycle and millions to billions of copies can be made after less than 30 cycles. Following amplification, the product is loaded into wells of an agarose gel and electrophoresis method is used for signal generation.

PCR has become a powerful tool for identification of infectious disease and biological agents [52]. Further modification of the basic PCR method mainly in the assay technique has been proposed. These are colorimetric enzyme immunoassay method (PCR-EIA) and fluorogenic 5' nuclease PCR assays. Lawrence Livermore laboratory has adopted these assays in to a miniaturized analytical thermal cycling instrument (MATCI) to shorten the performance time. The PCR-EIA is found to be at least 10 times more sensitive than standard PCR and the other

methods described above. In Table 9.3 are given a comparison of these methods for *Y. Pestis* agent.

Table 9.3 Comparison of sensitivity of various PCR format for *Y. Pestis* [53].

	Performance Time	Limit of Sensitivity	Specificity (%)
Standard PCR	2-3 hr	300 copies	100
PCR-EIA	2.5-3.5 hr	30 copies	100
5' Nuclease PCR	2-3 hr	300 copies	100
MATCI	20-60 min	>300 copies	100

Immunoassay Based Identification Systems

An immunoassay depends on the highly specific binding (reaction) of antigens with their corresponding antibodies thus forming a complex. In this method the presence of an analyte is detected and identified based on the antigen-antibody binding reaction. The antibody has a Y shape structure consisting of two heavy chains and two light chains joined by covalent double bonds. The base of the Y is constant among antibodies, while the top of the Y is specific for a particular antigen forming the variable region (See Figure 9.21).

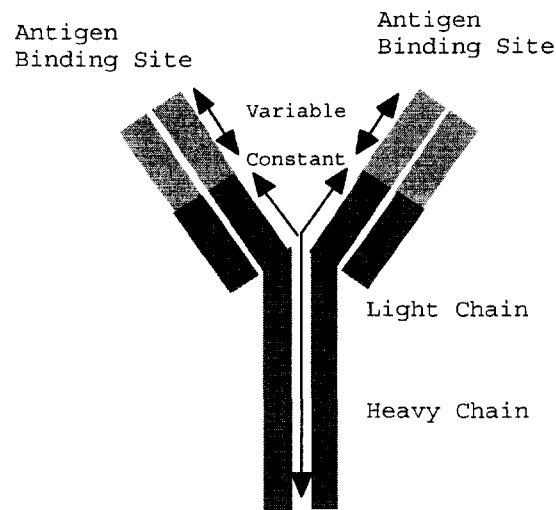


Figure 9.21 Antibody structure. Source: www.biology.arizona.edu/immunology/tutorials/antibody/structure.html [54].

The antigen is a foreign substance that triggers an immune response and may be a lipid, polysaccharide, or protein. The epitope is the site of the antigen, because the antibody does not generally recognize the whole antigen, detected by the antibody. Each antigen may have several different antigenic determinants. The antibody attaches itself to the antigen. Each antibody is specific for one antigenic epitope. The antibody-antigen binding may be shown schematically (Figure 9.22).

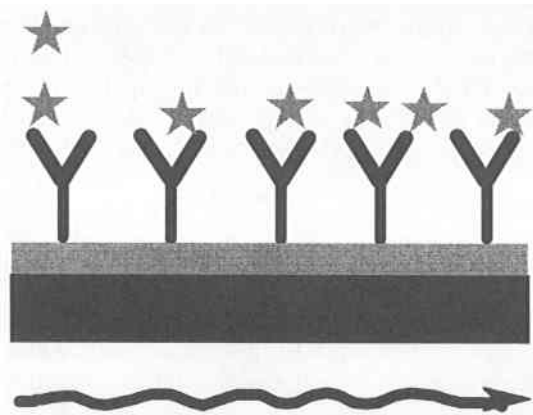


Figure 9.22 Antibody-antigen binding.

A number of detection methods have been developed based on immunoassay technology. These methods are described in the following pages.

Hand Held Immunochromatographic Assays (HHA)

The HHA is a simple, antibody-based assay that can be used to identify a variety of biological warfare agents. HHAs are inexpensive and very reliable. HHAs are designed to identify one agent per assay. There are two types of HHAs; the chromatographic type and flow-through assay type.

In the chromatographic type, a membrane strip is printed with three lines: (1) detector antibody coated blue latex particles, (2) biological agent capture antibody and (3) a reaction control of antibody directed to the antibody on the blue latex particles. The triple coated membrane strip is dried and is mounted into a ticket. To detect the presence of a biological agent, a small portion of liquid sample containing the suspected agent is placed in a well on the assay. The solution wicks through the assay where it is successively exposed to different antibodies. If antigen is present, a complex is formed and is captured by the biological-agent-capture antibody and a line appears in the test window (T). A line will also appear at the site of the reaction control window (C). Appearance of a line in this region only indicates that the antibodies are behaving properly but is not an indication of exposure to the biological agent. Therefore, a positive assay will have two lines,

one in each window. A negative assay will have only one line in the reaction control window (C). On average it takes 15 minutes to complete the assay. A shorter exposure time could give false negative results and a longer time may give false positives as the labeled antibody can start to flow back down the assay. The colored indications are not permanent and will fade quickly with time. To overcome the lack of sensitivity and occasional false positive of traditional HHAs, the U.S. Army Soldier and Biological Command (SBCCOM) and the U.S. Army Research Laboratories are investigating dendrimer-based tickets. So far, a variety of nanostructured polymeric materials have been synthesized and tested. Among them, the rigid, spherical, tree-like dendrimers are the best nanostructured polymers capable of orienting the antibody binding direction at different surfaces. As a result, HHA tickets have been significantly enhanced, and the detection time has been dramatically shortened.

Flow Through Assay

Hand held immunoassay can be also carried out in a flow through mode. The ticket, which is a plastic container, consists of a sample well with an absorbent pad backing to the membrane. In order to perform a test, the liquid sample suspected of containing the agent is introduced into the sample well. Antigen in the sample is captured on the membrane. A second reagent solution is added to the

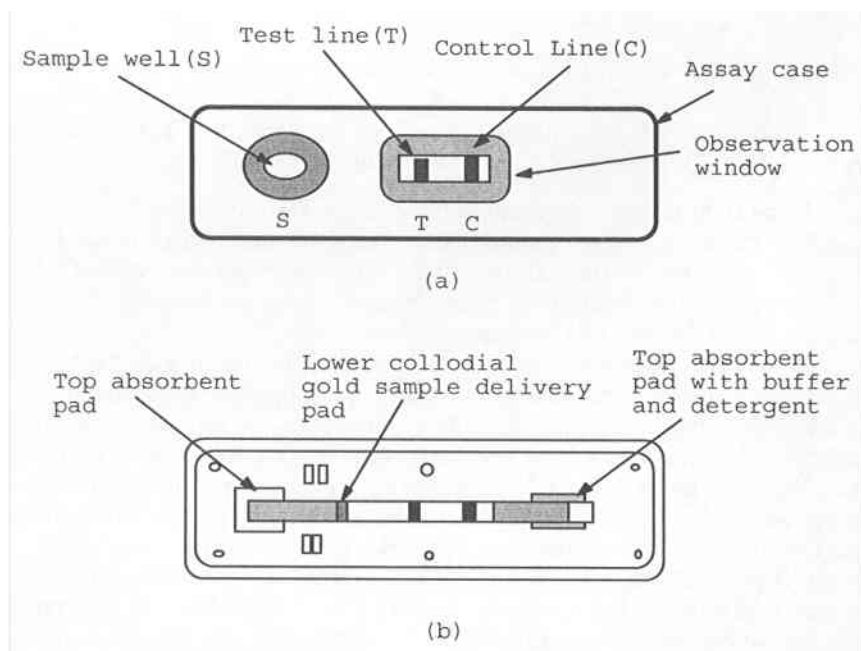


Figure 9.23 A hand held immunoassay ticket: (a) cover on, (b) cover removed.

added to the same sample well and it also flows through the membrane surface. The reagent solution contains an indicator antibody tagged with colloidal gold as an indicating agent. When the tagged antibody binds with the antigen on the membrane surface, a red spot is produced. Generally a reaction control antibody is bound in a horizontal strip on the membrane whereas the specific anti-agent antibody is bound in a vertical strip. If a red "minus sign" appears every time a test is conducted, it confirms the validity of the test. A red "plus sign" indicates the presence of the biological agent.

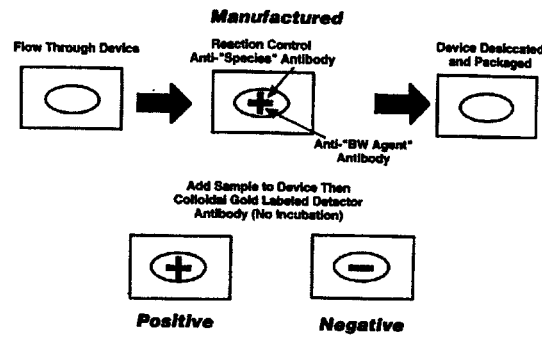


Figure 9.24 A flow through assay system.

Smart Tickets

Sensitive Membrane Antigen Rapid Test (SMART)TM is a registered trademark of New Horizons Diagnostics Corporation. The SMARTTM identification tickets are self-contained, colorimetric, and are based on solid-phase immunofiltration assays designed to be used in conjunction with a liquid interface. SMARTTM tickets are capable of detecting both endospore-forming bacteria and proteinaceous toxins or soluble antigens, including bacteria. The detection is accomplished by targeting the antigen in the sample that binds with antibody tagged with colloidal gold labeled reagents. Antibodies specific to the agent of interest are conjugated to colloidal gold particles. When concentrated on solid surfaces, these particles can be seen by the naked eye. Labeled antibodies can easily be lyophilized and reconstituted without losing activity or specificity. The presence or absence of the target antigen is indicated colorimetrically. A small red dot appears on the ticket that the user compares with a color chart. The older version of SMARTTM tickets that were used during the Gulf War tends to provide a higher percentage of false positives. The reliability of this method has been improved significantly by employing a lateral flow system. In lateral flow devices the chemical reagents are separated across the test strip. This lateral design provides fewer false positives in environmentally collected samples. The diagnostic kits are

available for anthrax, cholera, ricin, staph enterotoxin, *Y. Pestis*, tularemia, and botulism toxin [55].

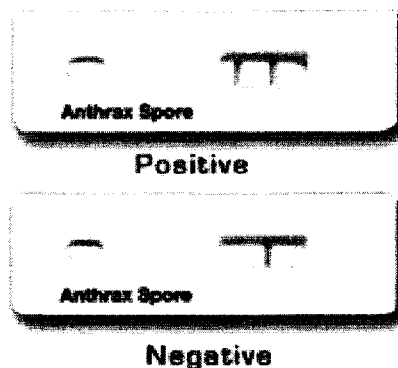


Figure 9.25 A SMART™ ticket for anthrax detection.

Electrochemical Luminescence

The ability of certain molecules such as ruthenium (II) tris(2,2'-bipyridine) (RUBY32+) to emit light or to luminesce has been utilized to detect antibody-antigen binding of the biological agent. If the light is produced by a chemical reaction, it is called chemiluminescence. If the chemiluminescent reaction is initiated by an electrical stimulation of the molecules, it is then called ElectroChemiluminescence (ECL).

A typical ECL sandwich assay takes place in the following manner. A sample is mixed with a reagent containing biotinylated TSH antibody and a second ruthenium conjugated TSH antibody. Antibodies capture the TSH present in the sample in this step. The captured antibody is immobilized on streptavidin-coated paramagnetic microparticles. The biotinylated TSH antibody attaches to the streptavidin-coated surface of the microparticles. The antigen forms a sandwich with these two reagents. The solution is next drawn into the ECL measuring cell along with a buffer solution containing tripropylamine (TPA). A magnet located under the electrode captures the microparticles in a thin, even layer on the electrode's surface. The magnet is removed and voltage is applied to the electrode. The association of TPA and the electrode results in a fast electron transfer reaction. This transfer initiates the excitation of the ruthenium (II) tris(2,2'-bipyridine) (RUBY32+) molecule which results in a emission of a photon at 620 nm. The ECL reaction occurs only if the antigen is present. This process also regenerates the ruthenium complex, which can perform multiple cycles during the measurement. The result is amplification of the signal. Multiple readings are taken by the photomultiplier tube (PMT) and the readings are integrated and compared to the

calibration curve to obtain a quantitative result. Regeneration of the electrode surface is accomplished by controlled variation of the electrode potential. The ECL measuring cell is then ready for another measurement. The process for detecting the biological agent is shown in Figure 9.26. Although the very first measurement takes about 17 minutes, subsequent measurements can be obtained in one minute. A general review of the chemiluminescence immunoassays process was provided by Rongen et al. [56] and Bowie et al. [57]. Yu et al. [58] have used the electrochemiluminescence assay for detection of biological threat agents. Results of detecting several biological agents by electrochemiluminescence is shown in Table 9.4. Yu et al. [58] concluded that electrochemiluminescence is a sensitive and effective means to detect biological agents from various matrices.

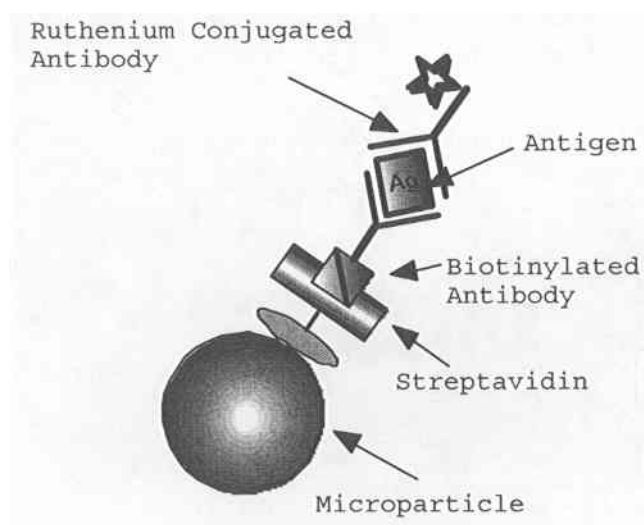


Figure 9.26 Schematic of electrochemiluminescence assay process.

Source: <http://us.labsystems.roche.com/ecl/ecltech.htm>.

Table 9.4 Results of detection of various biological agents by electrochemiluminescence method [58].

Biological Agent	Detection Limit
Staphylococcal enterotoxin type-B	0.5 pg/ml
Bacillus Anthracis	0.001 cfu/ml
Bot A	4 pg/ml
Cholerae toxin B	2 pg/ml
Ricin A chain	0.5 pg/ml

Light-Addressable Potentiometric Sensor

The Light-Addressable Potentiometric Sensor (LAPS) consists of an array of semiconductor devices, on top of which the biological agents are immobilized. The LAPS comprises an Electrolyte-Insulator-Semiconductor-structure (EIS), where a bias potential can be applied between an ohmic contact at the backside of the semiconductor and a reference electrode in the electrolyte.

By illuminating parts of the surface of the device with a beam of light, an electrical potential is generated between thin gold layers on the surface of the insulator located under the membrane filters. Therefore surface potentials can be measured in a spatially resolved manner, by scanning the light-pointer across the surface of the device. A number of biochemical events occurring simultaneously on the surface can be measured.

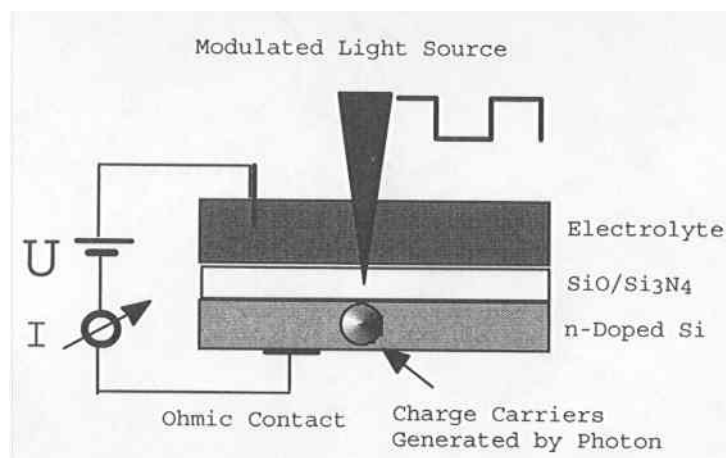


Figure 9.27 A typical LAPS system [59].

A typical LAPS sandwich assay is shown in Figure 9.27. The complete process may be divided into three stages; (1) reaction stage, (2) separation stage, and (3) detection stage.

In the reaction stage, the labeled antibodies, the sample containing the analyte, streptavidin, and anti-fluorescein/urease conjugate are combined together to form the first reagent. If antigen is present in the sample the sandwich reaction occurs in the solution.

The reaction product is transferred onto a nitrocellulose biotinylated membrane filter by filtering the solution through the membrane. The strong affinity of streptavidin for biotin is used to capture and concentrate the reaction complexes onto a biotinylated membrane filter and is called the separation stage (See Figure 9.28)

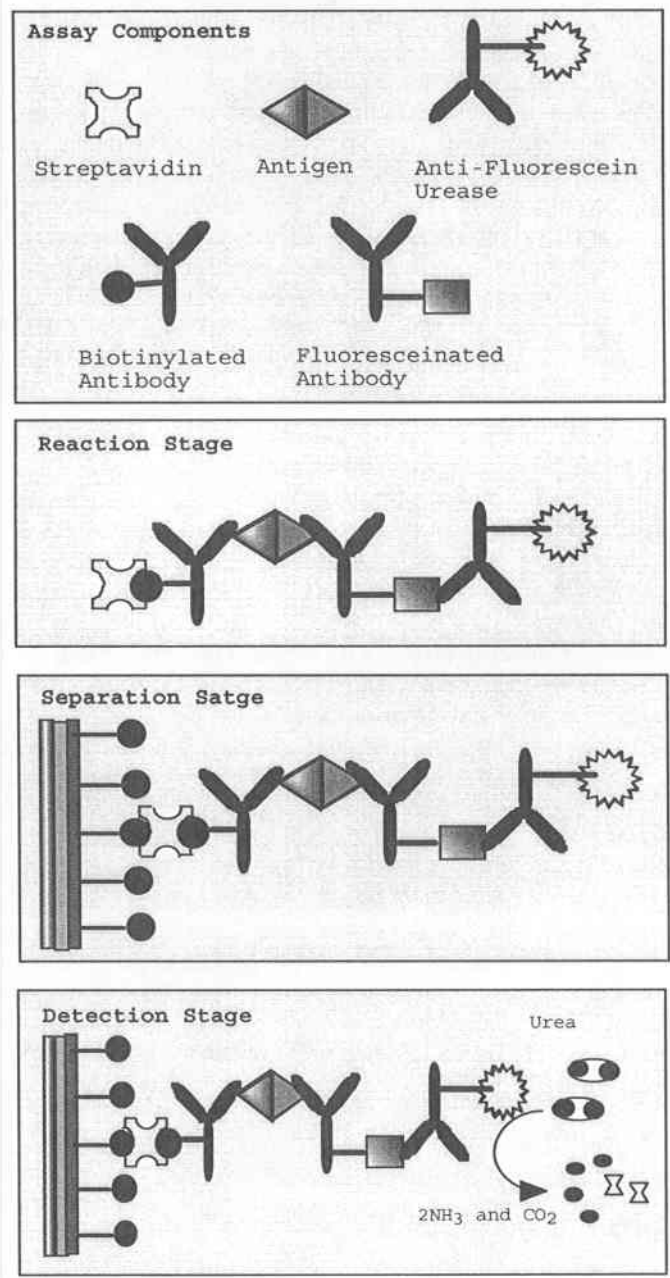


Figure 9.28 Schematic of LAPS immunoassay process [60].
 Source: www.moleculardevices.com/pages/thresh_ila.html.

A labeled anti-fluorescein urease antibody which binds to the fluorescein label on the previously captured complex is filtered through the same membrane. The detection is accomplished by placing this membrane filter into the reader, which contains the substrate urea and the light-addressable potentiometric sensor (LAPS). Inside the reader, urea is hydrolyzed by urease, producing a pH change due to the enzymatic activity at the silicon sensor surface.

The US Department of Defense has implemented a Biological Integrated Detection System (BIDS) for providing early warning and detection of biological threat agents in a battlefield. In the BIDS the biological detection system employs a LAPS and a flow through immunofiltration enzyme based assay system. As indicated by Uithoven et al. [61], the LAPS system was tested using *Bacillus subtilis* spores in the concentration range of 10^4 to 10^6 cfu/ml. The limit of detection was 3×10^3 cfu/ml for *B. subtilis*.

Fluorescent Evanescent Wave Fiber Optic Immunosensor

In this technology, antibodies are immobilized on the surface of either a glass optical fiber, a plastic cylindrical waveguide, or a planar waveguide. The antibodies bind fluorescently labeled analytes in a test sample and the antigen-antibody binding is detected using the fluorescent tag approach. The bound label should be within the evanescent wave zone. The input light excites the fluorescently labeled analyte resulting in a fluorescence signal. A fiber optic waveguide is used to confine and direct light along its length. The basic design of an optical fiber consists of two components - the core and the cladding. Core and cladding differ primarily in the refractive index of the glass. The core's refractive index is slightly higher than the cladding's, thereby creating a boundary for a circular waveguide. The biosensor is created by removing (i.e., etching away) the fiber clad material and the exposed core glass is coated with an unlabeled capture antibody. The coated fiber core is exposed to the analyte to which a second fluorescently labeled antibody is added. Molecular species can interact with the evanescent wave radiation as the analyte-antibody complex now act as the cladding or lower refractive index medium. The nature of the evanescent wave is such that it interacts only with the molecular species that lie within its penetration depth. Antigens and fluorescently labeled antibodies form a sandwich immunocomplex with the immobilized antibody. This immunocomplex lies within the evanescent zone, and the evanescent wave interact with the fluorophores and the resulting fluorescence is coupled back into the fiber and can be detected from a distance.

A fiber optic sensor in general will consist of a source of light, a length of sensing (and transmission) fiber, a photo-detector, demodulator, processing and display optics and the required electronics. A schematic diagram of one channel of a multi channel fiber optic based evanescent wave fluorescence sensor is shown in Figure 9.29. Generally a near infrared diode laser is used for the light source. The input fiber light is coupled into the dual-tapered sensing fiber and travels down the tapered fiber length. Tapering the fibers enhances the amount of fluorescence that can be coupled back into the fiber and therefore increases the signal. If the tagged

antibody is present which constitutes the presence of biological agent or a positive test, the input fiber light excites fluorescence from the special fluorescent dye tag, cyanine 5. Antigen concentration can be determined based on the intensity of fluorescence at a certain point. This fluorescent light travels back down the sensing fiber and is collected by standard return fiber. A schematic diagram of a evanescent wave fiber optic immunosensor is shown in Figure 9.30.

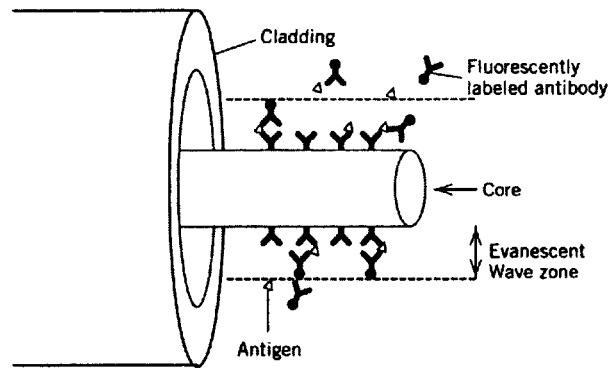


Figure 9.29 Antibodies immobilised onto the exposed core of an optical fiber bind antigens in solution, concentrating them within evanescent sensing zone [62].

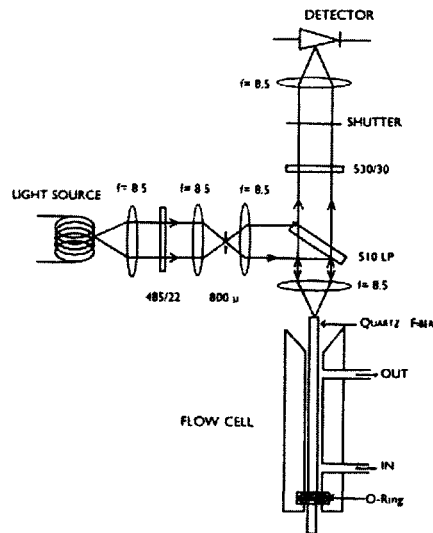


Figure 9.30 Schematic diagram of a evanescent wave immunosensor [63].

Research International Corporation has developed a portable automated fiber optic biosensor, called RAPTOR, for detection of biological threat agents. It performs rapid (3 to 10 minute), fluorescent sandwich immunoassays on the surface of short polystyrene optical probes for up to four target analytes simultaneously. The optical probes can be reused up to forty times, or until a positive result is obtained, reducing the logistical burden for field operations. Numerous assays for toxins, such as SEB and ricin, and bacteria, such as *Bacillus anthracis* and *Francisella tularensis*, have been developed. Research International has commercialized the RAPTOR, and development of a second-generation instrument, sponsored by the US Marine Corps, is now in progress [64].

Table 9.2 Limits of detection for toxins and pathogens using a 10-minute assay performed with RAPTOR [64].

Biological Agents	Type	Limit of Detection
Staphylococcal enterotoxin B(SEB)	Toxin	1 ng/ml
Ricin	Toxin	10 ng/ml
Cholera toxin	Toxin	1 ng/ml
<i>Yersinia pestis</i> F1	Bacterial surface protein	10 ng/ml
<i>Bacillus anthracis</i>	Gram positive bacterium (vegetative form)	50 cfu/ml
<i>Bacillus globigii</i>	Gram positive bacterium (spore)	5×10^4 spores/ml
<i>Brucella abortus</i>	Gram negative bacterium	7×10^4 cfu/ml
<i>Francisella tularensis</i>	Gram negative bacterium	5×10^4 cfu/ml
<i>Giardia lamblia</i>	Protozoan cysts	3×10^4 cysts/ml

No-Tag Biosensors

A number of sensors have been developed or are under development that do not need to form a sandwich assay. Antigen-antibody binding is detected directly so no tag reagent is required. Advantages to this type of assay include simplification of the analysis process (fewer steps, fewer components), minimized disposable fluid use (no need to carry tag reagent solutions), reuse of sensors after a negative test (minimal disposable use), and a smaller, lighter-weight instrument that consumes less power. Examples of no-tag biosensor methods include interferometry, surface plasmon resonance, piezo-electric crystal microbalance, waveguide coupler, and electrical capacitance. These methods are briefly described below.

Surface Plasmon Resonance

Several biosensors have been developed based on the phenomenon known as Surface Plasmon Resonance, which is a quantum optical-electrical phenome-

non arising from the interaction of light with a metal surface. Under certain conditions the energy carried by photons of light is transferred to packets of electrons, called plasmons, on a metal's surface [65, 66]. Energy transfer occurs only at a specific resonance wavelength of light: the wavelength where the quantum energy carried by the photons exactly equals the quantum energy level of the plasmons.

SPR sensors generally use a 50 nm thick gold coating on a plastic support. Three types of surface structures are used in SPR based sensors: the surface of a right angle prism, a sub-micron sinusoidal grating molded into the plastic surface, and optical waveguide based system.

Gold is used since it does not oxidize easily and therefore the surface chemistry or properties are not affected. The gold is subsequently coated with binding molecules. The binding molecules may be antibodies, DNA probes, enzymes or other reagents that can react exclusively with a specific analyte.

The coated metal surface interacts with light at a characteristic resonant wavelength that depends upon the molecular composition at the metal's surface. When the coated metal is exposed to a sample that contains analyte, the analyte binds to the metal through its specific interaction with the binding molecules. As an analyte is bound, the composition at the surface changes and consequently the resonant wavelength shifts. The magnitude of the change in the resonant wavelength is proportional to the amount of binding that takes place, which is proportional to the concentration of the analyte in the sample. In the SPR system, the binding events are monitored in real-time and it is not necessary to label the interacting biomolecules (See Figure 9.31).

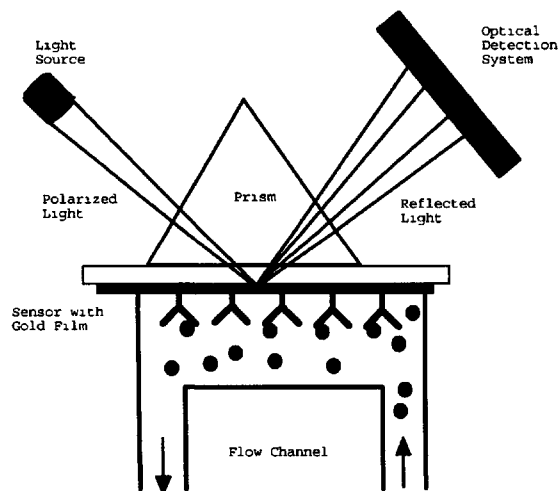


Figure 9.31 Principle of operation of a surface plasmon resonance biosensor.

Source: www.xantec.com/html/spr.html [67].

Interferometer Biosensor

Several biosensors are developed based on the interferometry principle that measures the change in refractive index on the surface of a planar single mode waveguide. An antibody coating is applied to the waveguide sensor's surface and its binding with antigen changes the refractive index of the surface layer which in turn alters the velocity of light travelling in the waveguide through its evanescent field interaction. Various types of interferometers are available including Mach-Zehnder, dual mode, and polarization, all of which have a planar architecture. The phase change due to the change in refractive index with respect to a reference light beam is measured. A polarization interferometer utilizes two perpendicular polarized modes of laser beam to perform the immunoassay. A guided polarized light perpendicular to the surface (TM mode) that has a high degree of evanescent wave interaction with the sensor coating forms the active arm of the interferometer. A horizontally polarized light (TE mode) that does not interact with the coating is the reference arm. Antigen-antibody binding on the surface causes a phase shift to occur between the two light beams. The degree of phase shift is directly proportional to the change in refractive index which in turn is related to the degree of antigen-antibody binding. A schematic diagram of an interferometry system is shown in Figure 9.32 [68].

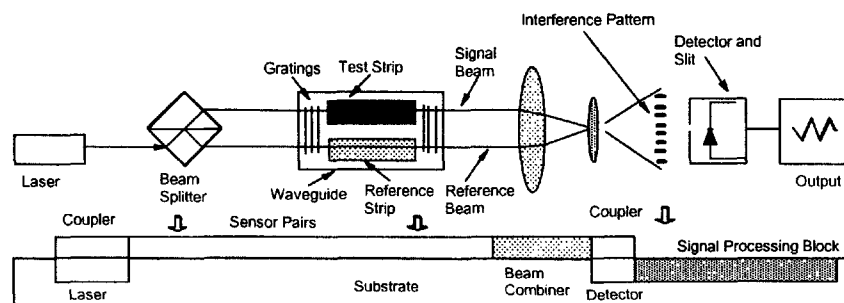


Figure 9.32 Interferometer setup and integration [68].

Piezoelectric Crystal Balance

The piezoelectric immunosensor is a very sensitive biosensor capable of detecting antigens in the picogram range. This type of device is believed to have the potential to detect antigens in the gas phase as well as in the liquid phase.

The antibody-antigen binding reaction deposits a small quantity of mass onto the surface of the oscillating piezoelectric crystal. This mass change results in a frequency change which is measured.

The most frequently used detector crystal for piezoelectric application is alpha quartz because they are insoluble in water and resistant to high temperatures. Alpha quartz crystals do not lose their piezoelectric properties up to a temperature

of 579°C. The resonant frequency of quartz crystal depends on the physical dimensions of the quartz plate and the thickness of the electrode deposited. Although both AT and BT-cut crystals are used as piezoelectric detectors, the AT-cut crystal is the most stable for construction of biosensors. The crystals usually take the form of discs, squares, and rectangles.

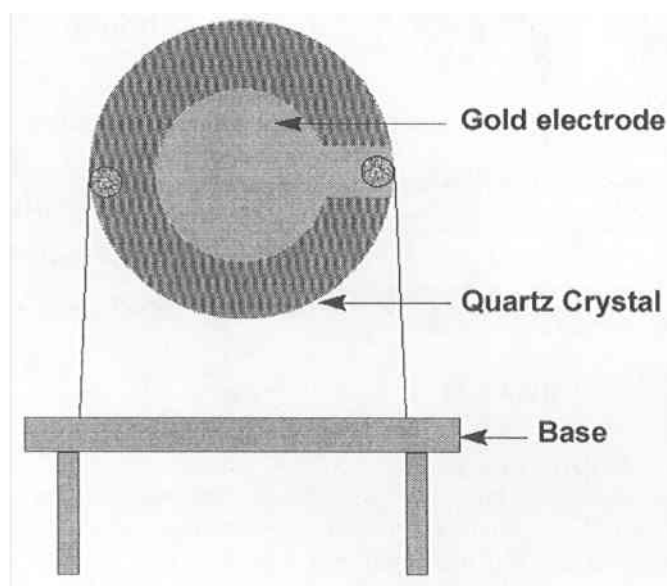


Figure 9.33 Piezoelectric biosensor.

Kumar [69] constructed a piezoelectric crystal biosensor using a 10 MHz AT-cut quartz crystal with an electrode coating deposited on each side using sputtering method. The crystal was mounted on a holder with stainless steel leads. A silver composite was used to connect the electrode to the wire. The crystals were 14 mm in diameter, and the electrodes on both sides of the crystal were 8 mm in diameter. Figure 9.34 shows the schematic diagram of a piezoelectric crystal biosensor. A flow cell can be used to introduce the sample, washing liquids, or buffer solutions to the sensing surface. Since no tag reagent is used, the sensor need not be replaced following a negative result. However, after a positive test, the sensor needs to be replaced.

Piezoelectric crystal sensors can be used for both gas and liquid phase [70]. Detection of biological warfare agents using Piezoelectric crystal sensors has been reported by a number of researchers [71]. Carter et al. [72] detected *Vibrio cholera* bacterium with an antibody based Piezoelectric crystal sensor. Later they used the same sensor for detection of ricin.

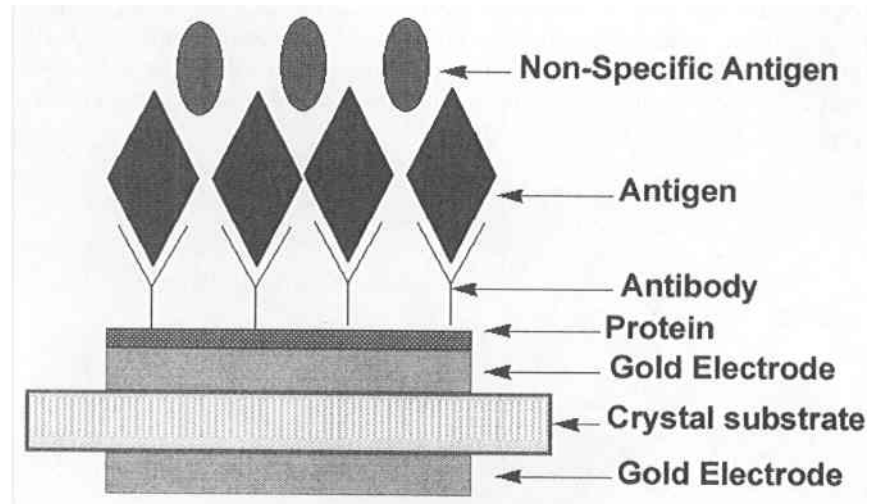


Figure 9.34 Piezoelectric immunoassay [69].

Resonant Mirror Biosensor

The resonant mirror biosensor combines an SPR sensor with the sensitivity of a waveguide device creating a highly sensitive yet simple device. The resonant mirror biosensor consists of four layers: the sensing surface, the high refractive index dielectric resonant layer, the low index coupling layer, and a prism. Polarised laser light illuminates the underside of the sensor surface at angles greater than the critical angle. The light is totally internally reflected and illuminates the detector array. A series of polarising filters are incorporated such that any light which follows this path is blocked before reaching the detectors. At one angle, called the resonant angle, a component of the light can couple through the low refractive index spacer layer and propagate along the high refractive index guiding layer. The angle where this coupling occurs, the resonant angle, is, essentially, dependent upon the refractive index at the surface of the sensor within the evanescent field. Hence, changes in refractive index [or mass] will change the resonant angle. So, as mass increases due to the binding at the binding surface the signal will increase, and as mass decreases at the dissociation surface the signal will decrease. This change in angle is linear with respect to mass. The fabrication of the resonant mirror is rather simple. Sputtering and ion beam assisted evaporation techniques are used to make the devices. Because of these methods, large quantities of uniform devices can be made inexpensively. A mirror arrangement is shown in Figure 9.35.

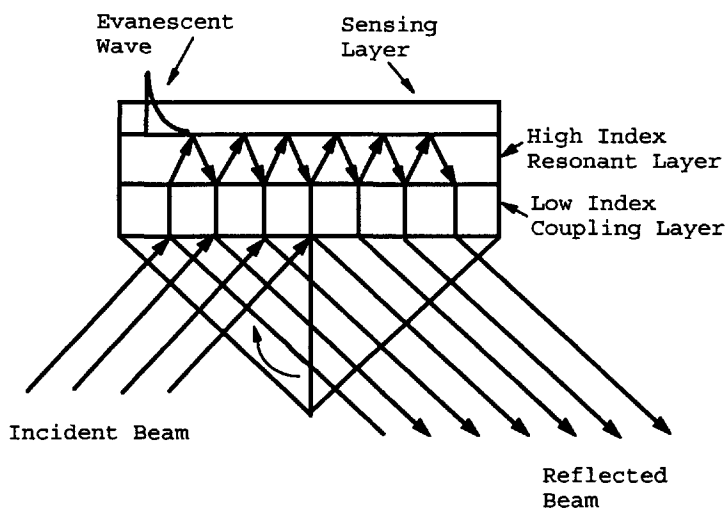


Figure 9.35 Resonance mirror arrangement [73].

Promising Technologies on the Horizon

Charged Based Deep Level Transient Spectroscopy (Q-DLTS)

QDLTS is discussed in Chapter 19, Chemical Weapon Delivery, Sensors and Detection Systems [74]. This unique technology is based on the ability to create a surface with a negative electron affinity by terminating the bonds on a diamond film surface with a halide [75]. This negative electron affinity causes the diamond surface to generate a positive charge which attracts polar molecules. The energy level of the molecule on the surface of the sensor is measured by flowing a transient current through the detector. The response of the molecule to this transient driver is unique. The method has been used with simple polar molecules. The sensitivity of the Q-DLTS technology is potentially in the sub-femtogram level.

Q-DLTS may be adaptable to existing systems that detect components of biological material such as lipids or may be used to directly detect the antigen.

Up-Converting Phosphor Technology

In this method, the phosphor particles are attached to detection probes, antibodies, or DNA that direct the phosphors to bind to biological agents. Upconverting phosphor materials emits visible light upon excitation with near infrared light rather than UV light. If the target antigen is present, an infrared diode laser causes

the phosphor probe to emit visible light. Some of the advantages of this methods are

- High sensitivity (single-phosphor particle)
- Many colors for multiplexing (10 unique colors currently)
- Robust, no photobleaching
- Diode laser excitation (compact sensors)

Spectroscopic Methods

Fourier transform infra-red spectroscopy (FTIR) and dispersive Raman microscopy can provide rapid identification of biological agents. The vibration of bonds within functional groups are used to identify as well as to quantify biochemical composition of the molecule. Goodacre et al. [76] used an Bruker IFS28 FTIR Spectrometer equipped with a mercury-cadmium-telluride-liquid nitrogen cooled detector to identify *E. coli* isolate Ea and *Proteus mirabilis* isolate Pa. The FTIR spectra of these two bacteria taken in diffuse reflectance mode is shown in Figure 9.36.

In Raman microscope, a laser illuminates the sample on a substrate and generates Raman scattering. The fingerprints of the sample is matched against a library of known fingerprints. The sample can be precisely identified by point-by-point matching of the fingerprints with the library data at all wavelengths. Dispersive Raman spectra of the same bacteria are shown in Figure 9.37.

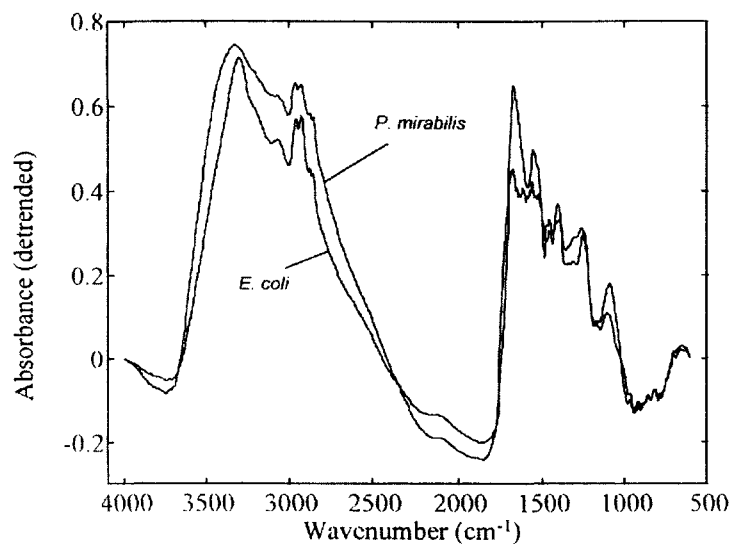


Figure 9.36 FT-IR diffuse reflectance absorbance spectra of *E. Coli* isolate Ea and *Proteus mirabilis* isolate Pa [76].

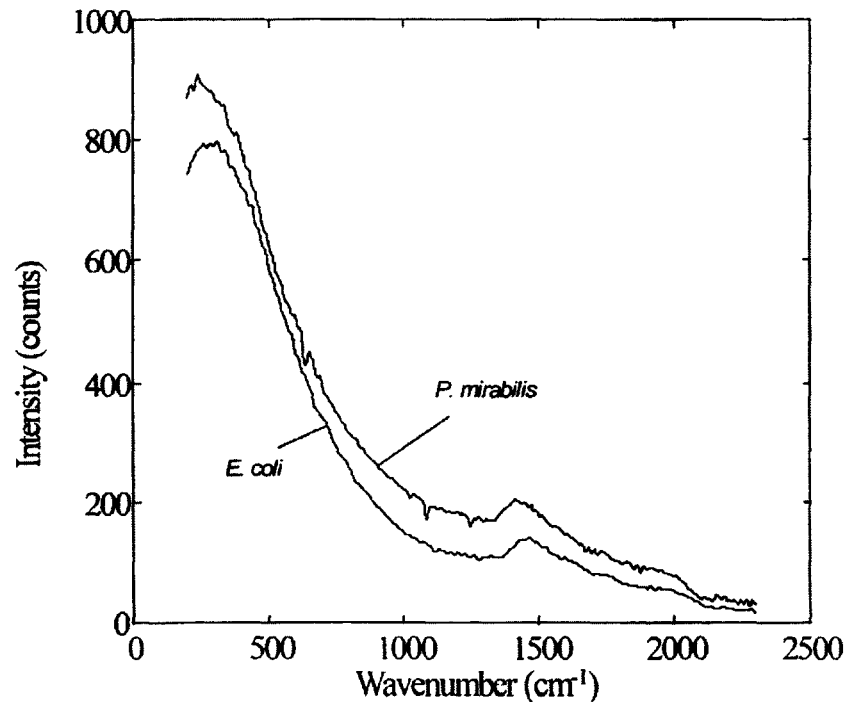


Figure 9.37 Dispersive Raman spectra of *E. Coli* isolate Ea and *Proteus mirabilis* isolate Pa [76].

CONCLUSION

Following the Persian Gulf War of 1991, significant improvement has been made in the field of biosensors. Not only have a number of new techniques been developed, but also the reliability and accuracy of the previous sensors have been improved considerably. However, it is likely that no one detection technology will meet all civilian needs as the number of potential threat agents for domestic terrorism are significantly larger than military use. The challenge with the biological detector is to achieve high sensitivity in the presence of large amount of interfering substances. Interference is generally due to the same physical parameter that is being used for selectivity, such as size, mass, or charge. One option may be to use multiple sensors, however, this can increase the cost significantly. Mobility and fieldability of the biological detection systems are also a major concern. Recently, a number of prototype units have designed with decreasing size and weight making them more mobile and fieldable.

REFERENCES

1. Biological warfare and detection capabilities. www.gulflink.osd.mil/faq_biologic_5jun.htm.
2. L Power, W Ellis, Jr. Pathogenic microbe sensor technology. Presented at the Defense Advanced Research Projects Agency Meeting on Bio-surveillance: Providing Detection in the New Millennium. Johns Hopkins University Applied Physics Laboratory, Laurel, MD, February 11, 1998. (As reported in Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response. Washington D. C.: National Academy Press, 1999).
3. TR Wehner, PD Stroud, WL May. Lidar detection of biological aerosols. Presented at the International Symposium on Optical Science Engineering, and Instrumentation Program on Remote Sensing, 4-9 August, Denver, CO, 1996.
4. Fibertek Inc., www.fibertek.com.
5. Military Analysis Network. <http://www.fas.org/man/dod-101/sys/land/lr-bsds.htm>.
6. R Foch. Micro unmanned vehicle. Presented at the Defense Advanced Research Projects Agency Meeting on Bio-surveillance: Providing Detection in the New Millennium. Johns Hopkins University Applied Physics Laboratory, Laurel, MD, February 11, 1998. (As reported in Institute of Medicine. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response. Washington D. C.: National Academy Press, 1999).
7. FS Ligler, GP Anderson, PT Davidson, RJ Foch, JT Ives, O King, D Keeley, G Page, DA Stenger, JP Whelan. Remote Sensing Using an Airborne Biosensor. *Environ. Sci. Technol.* 32 (16): 2461-2466, 1998.
8. CR Prasad, HS Lee, IH Hwang, M Nam, SL Mathur, B Ranganayakamma. Portable digital lidar: a compact stand-off bioagent aerosol sensor. *Proc. SPIE-Int. Soc. Opt. Eng. Chemical and Biological Sensing II.* 2001, pp 50-59.
9. KA Robertson, TK Ghosh, AL Hines, SK Loyalka, RC Warder, Jr., and D Novosel. Airborne Microorganisms: Their Occurrence and Removal. In *Indoor Air '90* Vol. 4, 567, 1990.
10. WC Hinds, *Aerosol Technology: Properties, Behavior, and Measurement of Airborne Particles.* John Wiley & Sons, Inc. New York, 1982.
11. WH Griest, MB Wise, KJ Hart, SA Lammert, CV Thompson, AA Vass. Biological agent detection and identification by the Block II Chemical Biological Mass Spectrometer. *Field Anal. Chem. Technol.* 5(4):177-184, 2001.
12. K Gotoh, H Masuda. Development of annular-type virtual impactor. *Powder Technol.* 118(1-2):68-78, 2001.

13. Y Ding, ST Ferguson, JM Wolfson, P Koutrakis. Development of a high volume slit nozzle virtual impactor to concentrate coarse particles. *Aerosol Science and Technology* 34(3):274-283, 2001.
14. CS Cox, CM Wathes. *Bioaerosol Handbook*. Lewis Publishers. Boca Raton. 1995.
15. FS Ligler, GP Anderson, PT Davidson, RJ Foch, JT Ives, O King, D Keeley, G Page, DA Stenger, JP Whelan. Remote Sensing Using an Airborne Biosensor. *Environ. Sci. Technol.* 32 (16): 2461-2466, 1998.
16. WD Griffiths, IW Stewart. Performance of bioaerosol samplers used by the UK biotechnology industry. *J Aerosol Science*, 30(8):1029-1040, 1999.
17. RG Pinnick, SC Hill, P Nachman, G Videen, G Chen, RK Chang. Aerosol fluorescence spectrum analyzer for rapid measurement of single micrometer-sized airborne biological particles. *Aerosol Sci Tech* 28:95-104, 1998.
18. SC Hill, RG Pinnick, S Niles, YL Pan, S Holler, RK Chang, J Bottiger, BT Chen, CS Orr, G Feather. Real-time measurement of fluorescence spectra from single airborne biological particles. *Field Anal Chem Tech* 3:221-239, 1999.
19. YL Pan, S Holler, RK Chang, SC Hill, RG Pinnick, S Niles, JR Bottiger. Single-shot fluorescence spectra of individual micrometer-sized bioaerosols illuminated by a 351- or a 266-nm ultraviolet laser. *Opt Letter* 24:116-118, 1999.
20. GW Faris, RA Copeland, K Mortelmans, BV Bronk. Spectrally resolved absolute fluorescence cross sections for bacillus spores. *Appl Opt* 36:958-967, 1997.
21. YS Cheng, EB Barr, BJ Fan, PJ Hargis, DJ Rader, TJ O'Hern, JR Torczynski, GC Tisone, BL Preppernau, SA Young, RJ Radloff. Detection of bioaerosols using multiwavelength UV fluorescence spectroscopy. *Aerosol Sci Tech* 30:186-201, 1999.
22. PH Kaye, JE Barton, E Hirst. Simultaneous light scattering and intrinsic fluorescence measurement for the classification of airborne particles. *Appl Opt* 39:3738-3745, 2000
23. J Ho. Real-time detection of biological aerosols with fluorescence aerodynamic particle sizer (FLAPS). *J Aerosol Sci* 27:S581-S582, 1996.
24. PP Hairston, J Ho, FR Quant. Design of an instrument for real-time detection of bioaerosols using simultaneous measurement of particle aerodynamic size and intrinsic fluorescence. *J Aerosol Sci* 28:471- 582, 1997.
25. LM Brosseau, D Vesley, N Rice, K Goodell, M Nellis, P Hairston. Differences in detected fluorescence among several bacterial species measured with a direct-reading particle sizer and fluorescence detector. *Aerosol Sci Tech* 2000;32:545-558.
26. GA Luoma, PP Cherrier, LA Retfalvi. Real-time warning of biological-agent attacks with the Canadian Integrated Biochemical Agent Detection System II (CIBADS II). *Field Anal Chem* 1999;3(4-5):260-273.

27. J Ho, M Spence, P Hairston. Measurement of biological aerosol with a fluorescent aerodynamic particle sizer (FLAPS): correlation of optical data with biological data. NATO ASI Ser., Ser. 1 Disarmament technologies (2000), 30(Rapid Methods for Analysis of Biological Materials in the Environment), 177-201.
28. JD Eversole, WK Cary, CS Scotto, R Pierson, M Spence, AJ Campillo. Continuous bioaerosol monitoring using UV excitation fluorescence: outdoor test results. *Field Analytical Chemistry and Technology*. 15(4): 205-212, 2001.
29. HM Davey, DB Kell. A Portable flow cytometer for the detection and identification of microorganisms. NATO ASI Series. 1. Disarmament Technologies-Vol. 30. Rapid Methods for Analysis of Biological materials in the Environment. Eds. PJ Stopa and MA Bartoszcze. 159-167, 2000.
30. PJ Stopa, H Kulaga, P Anderson, M Cain. Field applications of flow cytometry. NATO ASI Series. 1. Disarmament Technologies-Vol. 30. Rapid Methods for Analysis of Biological materials in the Environment. Eds. PJ Stopa and MA Bartoszcze. 137-158, 2000.
31. Biological Detection System Technologies. Technology and Industrial Base Study. A Primer on Biological Detection technologies. Prepared for the North American Technology and Industrial Base Organization, February 2001.
32. MW Mayo, SC Hill. Fluorescence spectra of bacteria, pollens and naturally occurring background. 3rd Workshop for Stand-off Detection for C and B Defence, VA, USA 105-112, Oct. 1994.
33. PP Hairston, J Ho, R Quant. Design of an instrument for real-time detection of bioaerosols using simultaneous measurements of particle aerodynamic size and intrinsic fluorescence. *J Aerosol Sci* 28:471-482, 1997.
34. RG Pinnick, SC Hill, P Nachman, G Videen, G Chen, RK Chang. Aerosol fluorescence spectrum analyzer for rapid measurement of single micrometer-sized airborne biological particles. *Aerosol Sci Technol* 28:95-104, 1998.
35. T Tjarnhage, M Stromqvist, G Olofsson, D Squirrell, J Burke, J Ho, M Spence. Multivariate data analysis of fluorescence signals from biological aerosols. *Field Analytical Chemistry and Technology*. 5(4): 171-176, 2001.
36. MP Sinha. Laser induced volatilization and ionization of microparticles. *Rev Sci Instruments* 55(6): 886-891, 1984.
37. MP Sinha, RM Platz, SK Friedlander, VL Vilker. Characterization of bacteria by particle beam MS. *Appl Environ Microbiology* 49(6): 1366-1373, 1985.
38. DN Heller, RJ Cotter, C Fenselau, OM Uy. Profiling of bacteria by fast atom bombardment mass spectroscopy. *Anal Chem* 59:2806-2809, 1987.

39. University of Melbourne Australia, School of Chemistry, Faculty of Science, <http://www.chemistry.unimelb.edu.au/MassSpec/homepage/electrospray.html>.
40. Electrospray ionization. www.methods.ch.cam.ac.uk/meth/ms/theory/esi.html.
41. R Zenobi, R Knochennuss. Ion formation in MALDI mass spectrometry. *Mass Spec Rev.* 17:337, 1998.
42. Review of Mass Spectrometry and Bioremediation Programs of the Edgewood Research, Development and Engineering Center, National Academy Press. Washington D.C., 1998.
43. JP Dworzanski, WH McClennen, PA Cole, SN Thomton, HLC Meuzelaar, NS Arnold, AP Snyder. Field-portable, automated pyrolysis-GC/IMS system for rapid biomarker detection in aerosols: A feasibility study. *Field Anal Chem Technol* 1:295-305, 1997.
44. AP Synder, A Tripathi, WM Maswadeh, J Ho, M Spence. Field detection and identification of a bioaerosol suite by pyrolysis-gas-chromatograph-ion mobility spectrometry. *Field Analytical Chemistry and Technology* 5(4):190-204, 2001.
45. SS Iqbal. MW Mayo, JG Bruno, BV Bronk, CA Batt, JP Chambers. A review of molecular recognition technologies for detection of biological threat agents. *Biosensors & Bioelectronics* 15:549-578, 2000.
46. VG Delvecchio, R Redkar, S Cheng, M Gress. Development of PCR-based assays for the detection and molecular genotyping of microorganisms of importance to biological warfare. *NATO ASI Ser., Ser. I* (2000), 30(Rapid Methods for Analysis of Biological Materials in the Environment), 219-229.
47. M Ibrahim, S Sofi, S Michelle, D Fishel, J Ezzell, E Henchal. Detection of biological agents using probe-based PCR assays. *Proc. ERDEC Sci. Conf. Chem. Biol. Def. Res.* (1999), Meeting Date 1998, 227-232.
48. G Franciosa, L Fenicia, C Cالدiani, P Aureli. PCR for detection of *Clostridium botulinum* type c in avian and environmental samples. *J Clin Microbiol* 34:882-885, 1996.
49. BN Clossais, S Minjolle, J Gicquel, R Colimon, PM Andre. Automated determination of amplified PCR products: application to HCV viremia detection and quantification. *Cell Biol* 41:959-966, 1995.
50. W Beyer, P Glockner, J Otto, R Boehm. A nested PCR method for the detection of *Bacillus anthracis* in environmental samples collected from former tannery sites. *Microbiol Res* 150(2):179-186, 1995.
51. MV Bloom. Polymerase Chain Reaction, Access Excellence, The National Health Museum. www.accessexcellence.org/RC/CT/polymerase_chain_reaction.html.

52. JE McDade, BE Anderson. Molecular epidemiology: application of nucleic acid amplification and sequence analysis. *Epidemiol Rev* 18:90-97, 1996.
53. EA Henchal, MS Ibrahim. Evaluation of polymerase chain reaction assays for identifying biological agents. NATO ASI Series. 1. Disarmament Technologies-Vol. 30. *Rapid Methods for Analysis of Biological materials in the Environment*. Eds. PJ Stopa and MA Bartoszcze. 239-249, 2000.
54. Antibody structure. Source: www.biology.arizona.edu/immunology/tutorials/antibody/structure.html.
55. New Horizons Diagnostics Inc. www.nhdiag.com/anthrax.shtml.
56. HA Rongen, RM Hoetelmans, V Bult, WP van Bennekom. Chemiluminescence and immunoassays. *J Pharm Biomed Anal* 12(4):433-462, 1994.
57. AR Bowie, MG Sanders, PJ Worsfold. Analytical applications of liquid phase chemiluminescence reactions-a review. *J Biolumin Chemilumin.* 11(2):61-90, 1996.
58. H Yu, JW McMahon, TM Campagnari. Detection of biological threat agents by immuno magnetic microsphere based solid phase fluorogenic and electro chemiluminescence. *Biosensors & Bioelectronics.* 14(10-11):829-840, 2000.
59. DG Hafeman, JW Parce, HM McConnell. Light-addressable potentiometric sensor for biochemical systems. *Science* 240:1182-1185, 1988.
60. Threshold System. Immuno ligand assay system. www.moleculardevices.com/pages/thresh_ila.html.
61. KA Uithoven, JC Schmidt, ME Ballman. Rapid identification of biological warfare agents using an instrument employing a light addressable potentiometric sensor and a flow through immunofiltration-enzyme assay system. *Biosensors & Bioelectronics* 14:761-770, 2000.
62. T McCormack, G Keating, A Killard, BM Manning, R O'Kennedy. Biomaterials and Biosensors. In *Principles of Chemical and Biological Sensor*. Ed. D Diamond, John Wiley & Sons, Inc. New York. 1998.
63. KR Rogers, JJ Valdes, El Defrawi. *Anal Biochem* 182:353-359, 1989.
64. GP Anderson, CA Rowe-Taitt, FS Ligler, RAPTOR: A portable, automated biosensor. *Proceedings of the First Conference on Point Detection for Chemical and Biological Defense*, Oct., 2000.
65. M McDonnell. Biosensors in the detection of biological agents. NATO ASI Series., Ser E, 252(Uses of Immobilized), 369-373, 1994.
66. RPH Kooyman, J Kolkman, J van Gent, J Greve. Surface plasmon resonance immunosensors: sensitivity considerations, *Anal. chim. Acta*, 213, 35 – 45, 1988.

67. SPR Basics. www.xantec.com/html/spr.html
68. D Kim, MA Brooke, NM Jokerst. Integrated Bio-Optoelectronic Sensor System. www.ece.gatech.edu/research/GTAC/Sp02PDFHandouts/DaeikKim.pdf.
69. A Kumar. Biosensors Based on Piezoelectric Crystal Detectors: Theory and Application. *JOM-e* 52(10), 2000. www.tms.org/pubs/journals/JOM/0010/Kumar/Kumar-0010.html.
70. JL Harteveld, MS Nieuwenhuizen, and ER Wils, Detection of staphylococcal enterotoxin B employing a piezoelectric crystal immunosensor, *Biosensors & Bioelectronics*, 12(7):661-7, 1997.
71. MS Nieuwenhuizen, J Harteveld, LN Johannes, K Gerritse. Detection of staphylococcal enterotoxin B employing a piezoelectric crystal immunosensor. Proc ERDEC Sci Conf Chem Biol Def Res Meeting Date 1998, 493-501, 1999.
72. RM Carter, MB Jacobs, GJ Lubrano, GG Guilbault. Piezoelectric detection of ricin and affinity purified goat anti-ricin antibody. *Anal Lett* 28:1379-1386, 1995.
73. Affinity Sensors, <http://www.affinity-sensors.com/faq.html>
74. V I Polyakov, AI Rukovishnikov, AV Khomich, BL Druz, D Kania, A Hayes, MA Prelas, RV Tompson, TK Ghosh, SK Loyalka. Surface Phenomena of the Thin Diamond-Like Carbon Films. Proceedings of the Materials Research Society 555: 345 1999.
75. M Prelas, G Popovici, LK Bigalow. Handbook on Industrial Diamond and Diamond Films. Marcell-Dekker. 1998.
76. R Goodacre, R Burton, N Kaderbhai, EM Timmins, A Woodward, PJ Rooney, DB Kell. Intelligent systems for the characterization of microorganisms from hyperspectral data. NATO ASI Series. I. Disarmament Technologies-Vol. 30. Rapid Methods for Analysis of Biological materials in the Environment. Eds. PJ Stopa and MA Bartoszcz. 111-136, 2000.

10

Bioterrorism: Preparation for Response – What the Government Can Do in Defending the Homeland

Marion C. Warwick

Missouri Department of Health and Senior Services, Jefferson City, and University of Missouri Medical School, Columbia, Missouri

INTRODUCTION

The field of response to bioterrorism is developing so rapidly that at best, this chapter will serve as a snapshot of the state of preparedness at the point in time just after the attacks on the World Trade Center and the Pentagon, and the establishment of the U.S. Office of Homeland Security.

This chapter begins with some background and explanation of the particular threats posed by the use of biological agents in warfare or terrorism, and introduces the importance of an efficient government response. From there the discussion proceeds in chronological order following the issues raised by a bioterrorism (BT) attack: prevention and deterrence, counteraction of each method of release and transmission, and the various elements of response that will be needed after an attack. The chapter ends with training, research, and conclusions, because they build on an understanding of the threats, and look forward to proactively mitigating them.

PERSPECTIVES ON THE USE OF BIOLOGICAL AGENTS AS WEAPONS

Epidemic disease evokes a primordial quality of dread disproportionate to that provoked by threats of equal magnitude from other causes [1]. Perhaps part of the reason for this is that infectious diseases have plagued mankind since antiquity [2]. They have played a pivotal though often overlooked role in the history of mankind, and there is no reason to believe that they will not continue to influence our history [3]. Today, human immunodeficiency virus (HIV), malaria, polio, measles and tuberculosis (TB), and other communicable diseases are threatening to cause massive individual suffering on an order of magnitude sufficient to threaten societal disruption in large parts of Africa and Asia [4]. At the same time, worldwide changes in societal practices, demographic patterns, and travel are enabling the emergence of new pathogens to which humans are immunologically vulnerable [5]. Given the delicate balance between the human race and microbes (mankind's historic enemy), why would anyone think to use biological agents as weapons?

Those who develop biological weapons have asked whether it, "is worse to die from a disease...than from bullets, bombs, or nuclear radiation?" and have argued that dying from disease is a "natural way of dying" [6]. In the sense that infectious diseases can cause death when deployed, they are no different from other weapons. However, mankind's repugnance of poison and unseen killers makes the use of biological agents particularly inhumane, and the use of an instrument that has historically been mankind's enemy seems to place the user on the side of the inhuman. Furthermore, unlike other weapons, infectious diseases are alive and hence not fully under the control of the person who wields them. Once released, they may spread and have effects reaching far beyond the original intent of those releasing them [7].

HISTORY OF BIOLOGICAL WARFARE

In spite of these concerns, biological pathogens, or living micro-organisms that cause disease, have been used since antiquity as weapons [8]. Biological warfare has been defined as "the use of micro-organisms and toxins, generally of microbial, plant, or animal origin, to produce disease and death in humans, livestock and crops" [9]. From a military point of view, paying attention to infectious diseases makes sense. Until the Russo-Japanese war, illness claimed more casualties in battle than inflicted by wounds of war [10].

The U.S. started its biological weapons program during World War II when it was believed that enemy states were developing them [11, 12]. Countries known to have had biological weapons programs include Japan [13], England [14], the former Soviet Union [15], South Africa [16], and North Korea [17]. Other countries suspected of past or present bioweapon development include Iran,

Syria, Egypt, Libya, Israel, and China [18]. Though the U.S. stopped its program in 1972, the Soviet Union's biological weapons program expanded throughout the 1980s and 1990s until recently [19]. Iraq may have an ongoing biological weapons program [20,21].

Today, widespread biotechnology and vaccine manufacture, requiring similar skills as for the production of biological weapons, increases the available facilities and the pool of expertise required for the manufacture of biological weapons. In addition, the Internet and encryption technology are decreasing the barriers to the production of weapons of mass destruction (WMD) by making knowledge available and allowing criminals and terrorists to communicate efficiently and anonymously [22]. However, the production of effective, biological agents as weapons may require better equipment and facilities than those usually available to small domestic groups [23].

THE WEAPONIZING PROCESS

Weaponizing is the process of modifying living micro-organisms to create deadly tools of war or terrorism [24] that differ from naturally occurring diseases in important characteristics. Biological weapons programs go through many stages to achieve such a final product [25, 26]. Out of thousands of possibilities, organisms with characteristics of durability and lethality are selected [27]. Biological weapons programs working independently in different countries have tended to select the same organisms, as there are a limited number of microbes that are both lethal and hardy enough to survive in the environment. Selecting the disease is not enough; diseases may have many strains which vary in their lethality. The Aum Shinrikyo cult responsible for the sarin gas attack in Tokyo in 1995 had also attempted releases of anthrax, which failed partly because they used a nontoxic strain of anthrax [28].

Once selected, the organisms are cultured in large quantities [29]. The fermenting tanks used for this stage vary in size from desktop models to huge vats several stories in height [30]. Whatever the size of production, the organisms in this wet form are not viable in the environment for long, are difficult to deploy, and therefore must be converted to a dry form for efficient use. Converting actively metabolizing organisms into a dry inactive form while also maintaining their viability is technically difficult [31]. Some programs have used freeze drying in this process. For aerosol dispersion, microorganisms are more effective if milled down to a particle size of between one and five microns. At this size they can evade the human upper respiratory tract defenses and be deposited in the lung when deployed.

The product at this stage is a deadly weapon, but it can be made even more deadly by removing electro-static charges [32]. Small charged particles tend to clump together or be drawn to dust fragments in the air. If the tiny particles are coated or mixed with inert material to remove the electro-static charges, they can

linger suspended in the air for longer periods of time and avoid clumping together. Once pathogens have gone through this weaponizing process they can infect exposed populations much more efficiently and in low dosages [33]. They may also cause different forms of disease. For instance, 95% of naturally occurring anthrax causes skin disease in which the organism enters the body through damaged skin. But anthrax that has been weaponized through all these steps can more easily cause the inhalational form of the disease. Weaponized micro-organisms must be handled carefully, to prevent illness among those working with them, and must be stored properly.

Various methods of dissemination are tested to assure that the microorganisms are able to withstand the dissemination process and remain viable enough to cause disease when the target is exposed. Most biological warfare programs test releases on animals [34], but human testing has also been performed. During World War II, some American conscientious objectors volunteered for testing in lieu of fighting [35], and a small unit in Japan tested its weapons on prisoners of war [36]. If “cocktails” or multiple biological agents were released simultaneously, the resulting mixture of diseases would make investigation of the outbreaks more confusing and difficult [37].

THE BIOLOGICAL WEAPONS

A list of diseases known to have been weaponized is presented in Table 10.1 [38]. Of the known weaponized agents, smallpox and anthrax pose the greatest threats [39], but for different reasons: smallpox is so contagious that its mortality rate of 30% kills large numbers of people; anthrax is not contagious but can have a mortality rate as high as 90% in its inhalational form, and it is very durable in the environment.

Smallpox has changed the course of history several times [40]. “Approximately 500 million people died of smallpox in the century that just ended. This compares with 320 million deaths during the same period as a result of all military and civilian casualties of war, cases of swine flu during the ruinous 1918 pandemic, and all cases of AIDS worldwide [41].” In his book, “Scourge: The Once and Future Threat of Smallpox” [42], Jonathan Tucker describes the ten year campaign which resulted, in 1979, in the first-ever eradication of a disease. This was a major triumph for public health and for humanity. Jeffrey Koplan, director of the Centers for Disease Control and Prevention (CDC), has commented, “It’s almost inconceivable that the incredible international human effort that went into eradicating smallpox could be overturned by malicious human acts...People subsumed all their differences working side by side to eradicate smallpox—Russians, Americans, Brazilians, Indians. In East Africa, wars were literally put on hold, and truces held, while everyone went into the field to get this done. It’s such a painful thing to consider that someone could use smallpox for a negative purpose, particularly when you are aware that it could cause hundreds of millions of deaths [43].”

Table 10.1 CDC's list of the BT diseases of most concern.

Disease	Biological Agent
CATEGORY A - high priority agents	
Smallpox	variola major
Anthrax	<i>Bacillus anthracis</i>
Plague	<i>Yersinia pestis</i>
botulism	toxin of <i>Clostridium botulinum</i>
tularemia	<i>Francisella tularensis</i>
hemorrhagic fevers	filoviruses: Ebola, Marburg arenaviruses: Lassa, Junin, others
CATEGORY B - second highest priority agents	
Q fever	<i>Coxiella burnetii</i>
brucellosis	<i>Brucella species</i>
glanders	<i>Burkholderia mallei</i>
Venezuelan, and eastern and western equine encephalomyelitis	alphaviruses
typhus	<i>Rickettsia prowazekii</i>
ricin toxin	from castor beans
epsilon toxin	<i>Clostridium perfringens</i>
staphylococcal enterotoxin B	<i>Staphylococcus species</i>
foodborne or waterborne disease agents	<i>Salmonella</i> , <i>Shigella dysenteriae</i> , <i>E. coli</i> 0157:H7, <i>Vibrio cholerae</i> , and <i>Cryptosporidium parvum</i>
CATEGORY C - emerging pathogens	
Pathogens that could be engineered for mass dissemination, such as Nipah virus, hantaviruses, tick-borne hemorrhagic fevers, and others.	

Source: Morbidity and Mortality Weekly Report, Biological and Chemical Terrorism, April 21,2000 / Volume 49 / No. RR-4, pp. 5-6

Today there are only two internationally legal repositories of the smallpox virus: at research facilities in the CDC in Atlanta, and in Vector, Russia. But

weaponized smallpox is known to have existed in Russia in large quantities (contrary to the Biological and Toxin Weapons Convention) as recently as 1992 [44].

Smallpox victims develop an extremely painful rash and a high fever. As smallpox is caused by a virus, antibiotics will not help. Antiviral medications do exist today, but as they were invented after smallpox had been eradicated, it is not known whether they would be effective against smallpox, though it is thought that one of them, Cidofovir, might be effective [45]. Smallpox is treated supportively (i.e. intravenous fluids, bedrest, and care of any complications that develop) without specific therapy, but today's supportive therapy may improve survival rates over those seen in the past.

The chief threat of smallpox is its ability to be transmitted from person to person and spread rapidly. It was eradicated in the last century by giving vaccine to everyone who had been in contact with a new case, as soon as the case was discovered. Contrary to most vaccines, the smallpox vaccine is effective even if given a few days after exposure to the disease. (This is a good example of how public health functions: not in treating individuals who are ill, but in interventions among well persons to prevent disease in the population). The production of vaccine has recently been accelerated, which will greatly improve our ability to cope with an outbreak. Controlling the spread of disease will be a first priority in response to a smallpox outbreak.

The signs and symptoms of the other BT diseases have been described elsewhere [46-49]. Biological weapons agents have unique differences from chemical and nuclear weapons of mass destruction. First, there is a time lag between release and symptoms, resulting in difficulty determining that an event has occurred as well as in uncovering the perpetrator and finding evidence of attribution [50]. Second, there is potential for secondary transmission causing expanding and unpredictable waves of new cases. Third, biological agents can be genetically manipulated, possibly leading to the creation of entirely new diseases.

THE ROLE OF THE U.S. GOVERNMENT

A 2001 GAO report [51] describes the federal agencies that have received funding for bioterrorism. Condensed descriptions from this report, along with a few other sources, have been included throughout the chapter in italics under the section most suitable, to demonstrate the breadth and complexity of government programs for BT.

Against BT, both in prevention and response, the government, as opposed to private citizens, must take the lead role. Though it is important that citizens understand and support the government, prevention involves international diplomacy, covert intelligence, research, and law enforcement, all governmental functions. Following a BT attack, needs would quickly overwhelm the resources of local hospitals, facilities, and supplies. The response to a large BT attack would require capabilities and expertise beyond the scope of any locality. Coordination

of local, state, and federal governments is needed to both develop and deploy the assets to contain and control a biological disaster.

The public can contribute to preparing for BT by becoming informed about the threats posed by BT, and supporting and advising the government in planning efforts. Knowledge can help individuals become mentally prepared; some may want to offer their services voluntarily in the event of an outbreak. An educated public will also help create the political will necessary to combat terrorism.

The Role of the Military

That biological warfare could be employed against military or civilian targets, overseas or in the homeland, raises questions about what role the military should have in defense of the homeland, and how it can best reorganize to meet new threats. The role of the military in civilian defense is limited by the Posse Comitatus Act of 1878, passed after the Civil War to restrict the government's ability to use the military in keeping civil order. However a 1984 disaster-relief law allows troops to respond to a national disaster at the President's order if they operate under the direction of the Federal Emergency Management Agency (FEMA) [52]. Other experts argue that in a crisis situation, pre-delegated legal authority may allow for military enforcement of civil laws even without special authorization from either the President or Congress [53]. If the homeland is attacked by foreign powers, it seems reasonable for the military to respond in defense. New doctrines, concepts, definitions, and strategies will need to be developed and articulated as the military adapts to its mission of civil support [54].

Several military units are working on plans to provide support to civil authorities in a terrorist incident: the U.S. Army Medical Institute for of Infectious Diseases (USAMRIID), the U.S. Army Soldier Biological and Chemical Command, the Director of Military Support, and the Joint Task Force for Civil Support (JTF-CS). The Joint Task Force for Civil Support (JTF-CS), part of U.S. Joint Forces command, is responsible for command and control of DOD Forces responding under the Federal Response Plan. JTF-CS engages in exercises, works with the Office of Emergency Preparedness (OEP) to develop plans for medical support to an incident, and also with FEMA to plan the deployment of Force Packages, or military response units that could also respond to an incident [55].

The Chemical Biological – Rapid Response Force (CBIRF), is a U.S. Marine Corps asset which can deliver technical expertise and equipment to the scene of a chemical or biological incident [56].

Other contributions of the military are described under the Surveillance, Mass Medical Care, and Research sections following.

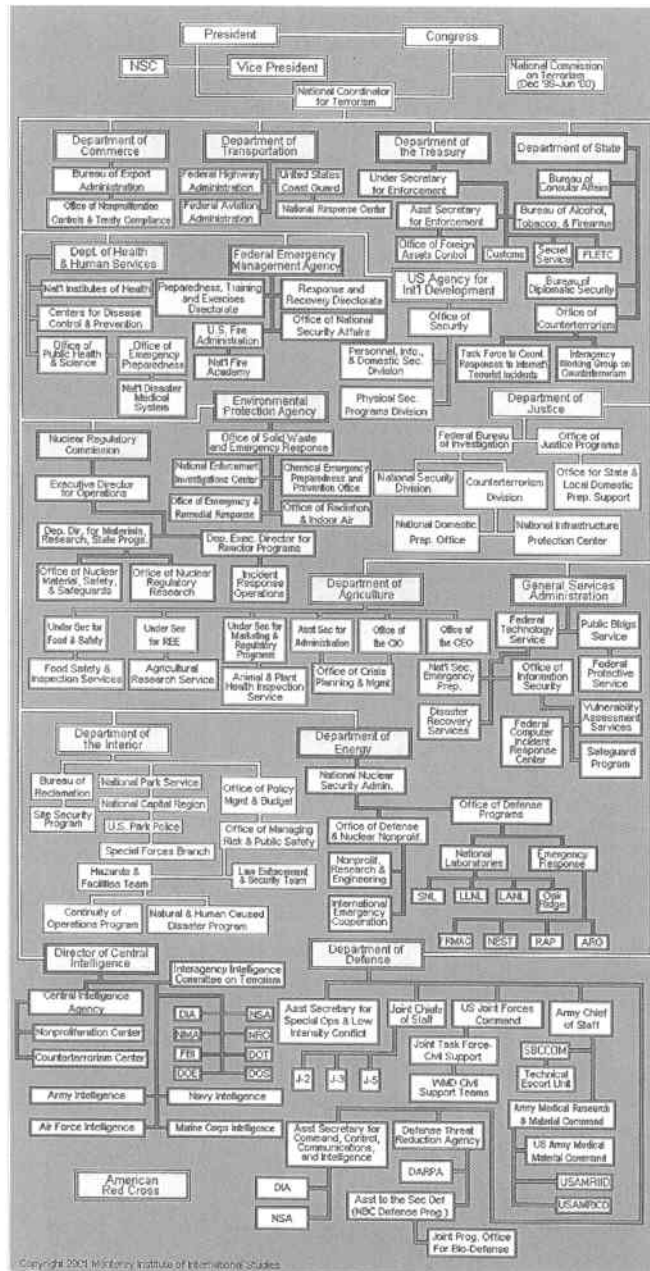


Figure 10.1 Organizational Chart for Terrorism Response.¹

¹ See Center for Nonproliferation Studies, Monterey Institute of International Studies <http://www.cns.mis.edu/research/cbw/domestic.htm> accessed 10/12/01.

The Federal Agencies

More than forty federal agencies have been involved in bioterrorism planning and could be involved in response to an attack as characterized in Figure 10.1 [57].

As evident from this, and another chart [58], the complexity of coordination that will be required of these agencies is daunting. Many GAO reports have described duplicative and uncoordinated government spending for BT [59, 60]. In order for these multiple resources to become assets they must be coordinated capably and efficiently.

Designation of an Overall Authority

Several important congressional reports, including the Gilmore Commission [61] and the Hart Rudman Report [62] and others [63, 64], have strongly recommended designation of an office with a high level of authority to help solve the problems of uncoordination and duplication of effort. This was accomplished in October, 2001, with the creation of the Office of Homeland Security [65]. This new office may be able to provide the direction needed to streamline government planning to eliminate duplication and to cover all aspects of bioterrorism preparation. What level of authority this Office will have, and whether it will become a cabinet agency have yet to be decided. Many argue that this position will need budgetary authority to accomplish the difficult task of reorganizing and streamlining government programs [66-68]. Command and control responsibilities, including legal authority, will need to be clarified to enable a coordinated federal response. Beyond that the federal plans need to be integrated with state and local plans [69]. Congressional oversight committees may also need reorganizing [70].

U.S. government plans for bioterrorism response have developed through a series of legislation and directives [71].

- The Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 1988, designates the National Security Council (NSC) as the principal forum for emergency policies. FEMA is to provide advice to the NSC based on coordination with other agencies at the federal, state, and local levels.
- The Federal Response Plan & Terrorism Incident Annex, April 1992, breaks down portions of emergencies into categories, and assigns responsibility for each to various agencies. Under this plan, Health and Human Services (HHS) is the lead agency responsible for the medical and public health response to BT.
- Presidential Decision Directive 39, June 1995, directs federal agencies within their areas of responsibility to reduce vulnerabilities, deter and respond to terrorism and WMD.
- Presidential Decision Directive 62, May 1998, clarifies the roles of agencies further, addresses cyber security, and establishes the Of-

office of the National Coordinator for Security, Infrastructure Protection and Counterterrorism to take the lead in developing guidelines for crisis management.

- The CONPLAN (Concept of Operations Plan), January 2001, provides overall guidance to agencies at all three levels of government on how the federal response will be coordinated.
- The National Security Presidential Directive-1 (NSPD-1), February 2001, designates the NSC Principals Committee as a forum for considering policy that affects national security and establishes the NSC Policy Coordination Committee to develop and implement policies for multiple agencies.

Under these directives the Federal Bureau of Investigation (FBI) is designated as the lead federal agency during the crisis phase and FEMA as the lead federal agency during the consequence phase of an event. These phases are meant to overlap and occur simultaneously.

Under the Federal Response plan, described above, HHS has the lead responsibility for medical and public health response to emergencies and terrorist incidents. A Special Assistant for Bioterrorism has recently been appointed within HHS to coordinate bioterrorism activities across the department [72]. The HHS oversees five agencies with responsibilities for on bioterrorism preparedness. The Agency for Healthcare Research and Quality (AHRQ), the Food and Drug Administration (FDA), and the National Institutes of Health (NIH) are mainly focused on research. The Office of Emergency Preparedness (OEP) and the Centers for Disease Control and Prevention (CDC) are focused mainly on consequence management [73].

Within CDC, the Bioterrorism Preparedness and Response Program (BPRP) coordinates bioterrorism planning internally and also administers BT funding for state health departments, which in turn, assist local health departments in BT planning and response. As federal authority among different federal agencies has been consolidated in the Office of Homeland Defense for WMD, one report has recommended that the BPRP, responsible for coordinating BT planning among the units within CDC, should be placed within the Office of the Director of CDC, and given budgetary authority [74].

The Role of State and Local Governments

Any bioterrorism outbreak on American soil would necessarily take place in a local jurisdiction somewhere; the local government would be responsible for handling the situation until help from state and federal governments arrives. The threats, resources, and capabilities of local governments vary widely. One thing they do have in common is a variety of agencies that could assist: most localities have fire, police, and public health departments, hospitals, and an office of the American Red Cross. The challenge local governments face is coordinating the

work of these agencies together. Most disciplines have close relationships with their state and federal counterpart agencies, but work very little with other agencies outside of their discipline, even though they are in the same locality. But an effective response from local governments will require local integration across the nation to streamline response and maximize capabilities across disciplinary lines.

States have further assets which can assist in an emergency, such as National Guard troops and state emergency management agencies. The governor of a state can declare a state emergency, and can request the president to declare a national emergency. State agencies coordinate between their counterpart agencies in federal and local levels of government and can offer assistance to local agencies when requested. State agencies face the same challenges of integration between agencies and disciplines described for federal and local governments.

PREVENTION

Deterrence is designed to prevent the development of a BT attack through creating disincentives; preemption stops a BT attack in process before any harm can occur.

Deterrence

Congress has passed legislation to deter the development of biological weapons. In 1989, the Biological Weapons Act was passed, which made the possession, sale, or manufacture of a biological substance "for use as a weapon" illegal [75]. In 1991, American companies were prohibited from commercial transactions with countries suspected of developing biological weapons, and in 1996 it became illegal to threaten to develop biological weapons. In 1997, 24 organisms and 12 toxins became designated as "restricted", requiring a permit to possess them [76].

Preventing programs from developing biological weapons would be ideal if it could be done. The Biological and Toxin Weapons Convention of 1972 [77] was meant to discourage nations from manufacturing biological weapons by international convention. As of December 2000, there were 143 states parties and 18 signatories to the Convention [78]. This has been controversial, and in 2000 and 2001 the United States was the sole nation holding up negotiations [79]. Some argue that treaties that cannot verify compliance are ineffective [80], that weapons inspections in Iraq failed to uncover existing programs, that positive scientific exchanges would be more effective [81], and that instituting more intrusive inspections would place confidential U.S. technological advances in jeopardy [82].

Proponents argue that abandoning an international agreement ratified by 110 nations with no other mechanism in place seems unwise [83, 84], and that enforcement may be an alternative way to strengthen the treaty [85].

Another concern is an estimated seventy thousand research scientists and technicians who had been employed in the biological weapons programs of the

former Soviet Union, and either lost their jobs or became underemployed [86] when these programs were dismantled. Their expertise would be desirable to those trying to develop biological weapons programs [87]. Opportunists may include transnational criminal organizations and others who would be willing to sell to the highest bidder, whether they are state or non-state actors [88]. There is also the possibility that biological samples from these programs may have been available to interested parties [89] through bribery or smuggling [90]. The United States has funded programs to find alternative work for those scientists [91, 92], and this funding should be continued.

Preemption

Preemption requires identification and location of an attack or delivery system and the capacity to disrupt it [93]. The roles of both foreign and domestic intelligence communities are critical in this regard, and mechanisms to provide better intelligence sharing and combined analysis are needed [94].

RELEASE AND TRANSMISSION

Before an organism or toxin can cause disease in a human, it must enter the body. Intact skin is an excellent barrier, which is why handwashing alone [95] may be highly effective in reducing the threat from specific BT agents, such as cutaneous anthrax. Organisms can enter the human body through any orifices, but the most likely portals of entry for BT are the nose [inhalation], the mouth [ingestion], and a break in the skin. Manufacturers of biological weapons are faced with the dilemma of releasing their product into the environment in such a way that humans will either inhale it, ingest it, or encounter it on a break in the skin. Different methods of release have been studied to achieve this purpose; each method or technology has inherent difficulties and advantages. Prevention and response plans must be tailored specifically to meet each method of transmission: air, water, food, zoonotic, agricultural, and others. Aside from an initial release, the prevention of subsequent spread of agents that are transmitted from person to person is also critical, and will require special planning.

Airborne Transmission

The airborne transmission route is often the most feared because of its potential for large numbers of casualties in both humans and animals [96, 97]. But as sunlight kills most organisms, and turbulent or high winds disperse the concentration of agents released in the air, airborne transmission is highly dependent on weather conditions. A clear, calm night with a slow steady air current [98] and an inversion with a layer of cold air trapping the release near the ground [99] are the best conditions for an airborne release in the outdoors. Biological weapons could

be released into the outside air by hand-held or other single point devices, or moving sources such as trucks and airplanes with modified spraying equipment.

In order to produce the small particles of one to five microns required to cause inhalational disease, specialized spraying equipment or other alterations would have to be retrofitted to airplanes. Air intake and air conditioning systems [100], or the internal air currents in subways could also be used to spread disease. The risk of a successful biologic attack by airborne transmission could be decreased by establishing procedures to limit access to items for specialized spraying, and by mandating standards for security of air-intake systems in public buildings, businesses, and private homes. Measures could include hepa filters, irradiation, and securing access. Until monitoring systems to detect the presence of pathogens in the air are available, there is little else that can be done to protect against an airborne release.

The Environmental Protection Agency (EPA) is responsible for the nation's air quality, and has capabilities for sampling and identifying environmental contaminants. It also plays a role in decontamination and long-term remediation. The EPA has 220 on-scene coordinators trained to respond to a hazardous material spill affecting the environment [101].

Waterborne Transmission

A safe water supply [102] in the United States has resulted in the near elimination of deadly water-borne diseases that still threaten many areas of the world: typhoid, cholera, and other diarrheal diseases. The three main elements of this system are supply, treatment, and distribution. Physical points of vulnerability include dams, aqueducts, pumping stations, and intake areas. Controlling human access to vulnerable points is difficult, but could be improved by incorporating intrusion sensors into existing disaster monitoring systems and increasing fences and other physical barriers. Since many portions of the water system are automated, measures must also be taken to guard against cyber attack.

Water supplies are difficult to contaminate because large quantities of contaminants would be required to obtain lethal concentrations and because chlorine kills most pathogens. Nevertheless, water systems may still be vulnerable to those biologic organisms for which only a small infective dose is required. If panic or anxiety is the goal, changing the color or taste of the water supply may be sufficient without actually introducing a toxic substance or achieving a lethal level of contamination [103].

One approach to improve water safety could focus on building greater versatility, redundancy, and inter-connectedness into the system, so that if one unit failed or became contaminated, water could be channeled from other units. Because existing water systems have evolved independently and are often fragmented, developing more broadly connected regional systems would require new collaboration, perhaps through mutual aid agreements for various assets such as water, equipment, and repair response. Other efforts should focus on better

monitoring devices for biological pathogens and toxins, and treatments capable of responding to them. Advances in water treatment technologies could be more widely applied, including sequential treatment in series when needed, to achieve a higher level of contamination removal [104].

Currently most public health communicable disease programs do not routinely collect information on the water supply of persons with waterborne diseases either at home or at work, yet this could be important for detecting problems related to a water source, whether municipal or private. Closer coordination between environmental and public health agencies could allow collection of these data and could further improve control of waterborne diseases.

The EPA is the lead agency for protection of the nation's water supply. For a bioterrorism incident involving the water supply, the EPA would work with CDC to design a response appropriate to each situation. The EPA is coordinating with the CDC to develop staff training for the biological aspects of its WMD response, and is creating methods to assess the vulnerability of water supply systems in conjunction with the Department of Energy (DOE) and the American Water Works Association Research Foundation [105].

Food Borne Transmission

The largest outbreak of bioterrorism to date was food borne, perpetrated in 1984 by a religious group that hoped to cause enough temporary illness in the community to influence local elections. They did not succeed, though 751 persons became ill through eating from salad bars contaminated with *Salmonella typhimurium*, a common food borne illness [106]. Fortunately, cooking kills most pathogens and deactivates many toxins.

The FDA's Center for Food Safety and Applied Nutrition is responsible for the safety of the food supply. In a collaborative effort, the CDC, the FDA, the United States Department of Agriculture (USDA), and nine state health departments have developed a program called FoodNet which provides more timely information on the occurrence of diseases which are likely to be food borne. The CDC has also collaborated with the FDA and USDA on another program called PulseNet, designed to improve the capability of state and federal laboratories to distinguish between subtypes of food borne bacteria in order to better characterize the extent of a given outbreak [107].

The FDA's Center for Food Safety and Applied Nutrition, responsible for monitoring and labeling the nation's food supply, has been preparing for bioterrorism involving food as a vector. It has developed a procedures manual used by health department workers in the investigation of food borne outbreaks [107].

The FDA's Center for Toxicological Research conducts research regarding the detection of various proteins in the food supply, including methods to determine their toxicity. The Center could bring this diagnostic capability to support a bioterrorism incident affecting the food supply. The Center has been developing

training materials in conjunction with FEMA and Arkansas public health officials [108].

Zoonotic and Agricultural Transmission

Zoonotic

Many of the bioterrorism agents are zoonotic diseases, that is, animals and humans can both be infected by them and transmission can occur between species. Thus, even if their occurrence is eliminated in humans, a reservoir of disease can remain among animals and wildlife that can be difficult to eradicate and will likely remain a potential source of infection for humans. Examples include anthrax [109], plague [110], tularemia [111], some of the viral encephalitides, brucellosis, and Q fever. To date animal and human health issues have been handled by separate government agencies that have little knowledge of each other's work. Effective bioterrorism planning will necessitate a coordinated approach between these agencies, even to the level of integrating data systems. Better integration of agencies with the responsibilities for veterinary and medical public health should be encouraged to address outbreaks that can affect both animals and humans [112].

West Nile disease is a viral encephalitis spread to humans by infected mosquitoes which also feed on horses and birds. Its spread across the country, tracked by testing of samples from birds and mosquitoes, reveals a slow progression westward, arriving in St. Louis in October 2001 [113], two years after it was first identified in New York City. Compared to other diseases, West Nile virus may not cause many fatalities, but because of its presence in the environmental ecosystem, it is here to stay.

Infected insects have been used as biological weapons. Though less effective than other methods [114], infected fleas can be grown in large quantities which cause disease when disseminated [115]. Since fleas infect rats, controlling rats helps to decrease the incidence of flea-borne diseases. Plague is an example of a BT disease spread by fleas in its naturally occurring form. Many local and state health departments have existing mosquito and rat control programs that would help to control the spread of some zoonotic diseases if they were ever released. Further study has been recommended to determine the effectiveness of these programs, and to identify new interventions [116].

Agricultural

Biological agents can be targeted specifically to affect crops and livestock to undermine economic progress and stability [117]. Countries are dependent on agriculture for food and economic health. In the spring of 2001, when an outbreak of foot and mouth disease occurred in the United Kingdom, "over 3.9 million livestock were slaughtered and an estimated 119,131,446 pounds [\$172,621,465] in indemnity payments were made during the campaign to eradicate foot and mouth disease" [118].

A recent Harvard University report lists recommendations for the USDA in improving the safety of animals and plants for BT attacks on four different levels [119]:

1. Organism Level. The USDA should be ready to supply vaccines for all (the most dangerous) foreign animal diseases.
2. Farm Level. The USDA should set up a Biosecurity Training Program to counter the threat of diseases and pests at the farm level.
3. Sector Level. The USDA should invest more resources in disease detection, surveillance, and diagnostic technologies. Examples include creating linked animal-human disease databases, developing more rapid diagnostic tests for foreign animal diseases, upgrading Plum Island (see below) to BL-4 (Biosafety level 4 is the highest level of safety, requiring laboratorians to wear protective gear and masks, and special circulation and treatment of air), and establishing a contingency network of veterinarians.
4. National Level. The USDA should be ready to deal with the public reaction to a serious food scare, and it should have the budgetary means to proceed with fast and efficient recovery.

These recommendations are similar to what is needed for human health.

The US Department of Agriculture (USDA) has an important role to play in the defense of attacks on plants and animals. The USDA monitors the Plum Island Animal Disease Center in New York, a research center with the laboratory diagnostic capability to detect unusual diseases in animals and plants. The USDA also houses the Animal and Plant Health Inspection Service, responsible for responding to the veterinary side of outbreaks of zoonotic disease. This Service has begun to develop educational materials and training programs for the recognition of biological weapons agents [120].

The FDA's Center for Veterinary Medicine regulates food additives and drugs given to animals, whether agricultural or domestic. In this capacity, the FDA has been collaborating with veterinary diagnostic laboratories and state officials to increase preparedness regarding risks to the food supply that could arise from biological terrorism directed against plants or animals [121].

Other Releases

Biological organisms can be engineered to corrupt materials such as the rubber in tires or synthetic materials, asphalt, and other kinds of plastics. These could cause both disruption and economic loss.

The U.S. Department of Transportation (DOT) oversees all civilian air, sea, and land transport within the United States, and also coordinates the safety of pipeline facilities. Through its National Response Center, staffed and housed by the Coast Guard, it serves as the point of contact for information regarding any

oil or other WMD materials released from transportation systems into the environment, and houses the National Response Team, a coordinating body composed of representatives from 16 federal agencies with responsibilities for response to an environmental emergency [122].

Secondary Transmission

If disease can spread beyond the site of initial release, carried to others by those infected from the first exposure, then it is said to be communicable or to have secondary transmission. Diseases with secondary transmission, such as pneumonic plague and smallpox, could spread outward in expanding waves, magnifying the initial release. To control communicable diseases, the treatment of individual patients needs to be combined with approaches to decrease transmission among the public. Strategies have been defined to decrease transmission from individual patients for both plague and smallpox, and would include wearing masks and taking antibiotics for plague [123], and vaccination and respiratory isolation with hepa masks and negative air pressure rooms for smallpox [124-126].

Measures to decrease transmission on a larger scale are more difficult to agree upon. The first major exercise of the federal response plan was called TOPOFF (for top officials) in May 2000, and simulated an expanding outbreak of plague. State public health officials who participated later made these observations:

The process of isolating patients until they are no longer contagious and identifying close contacts is typically straightforward. Isolation, however, was not possible during this exercise. The hospitals had too many patients and worried-well persons and too few health-care workers and empty rooms to permit isolation of pneumonic plague patients. As a result, an executive order was issued quarantining all persons in metropolitan Denver in their homes.

However, quarantining two million persons is not simple. Essential workers must be identified, be given prophylaxis and protective barriers, and be permitted to do their jobs. Other members of the community can stay in their homes only a few days before they need fresh supplies of food. Therefore, a one-time, blanket quarantine order is unlikely to be successful and cannot be enforced unless these and many other issues are addressed. The hospitals were quite demanding in their requests for reinforcements, and we made great efforts to assist them. However, by day three of the exercise it became clear that unless controlling the spread of the disease and triage and treatment of ill persons in hospitals receive equal effort, the demand for health-care services will not diminish. This was the single most important lesson we learned by participating in the exercise [127].

In another federal exercise called "Dark Winter" in June 2001 [128], senior officials over the course of two days walked through the major simulated decision points that could occur during a smallpox outbreak as it expanded rapidly to many states through person to person transmission. The exercise generated Congressional hearings, and together with its timing just prior to the attacks on the World

Trade Center, was influential in mobilizing government planning for smallpox and discussions on quarantine. A summary of “lessons learned” through interviews of the participants and Congressional testimony included the following points [129]:

1. Senior decision-makers trained in national security and defense matters are unfamiliar with issues surrounding BT attacks.
2. A lack of information systems with real-time data in the medical and public health communities would confront decision-makers with many uncertainties.
3. An insufficient supply of smallpox vaccine would limit options to control an outbreak, and could cause disagreement about disposition of existing vaccine.
4. The medical care system lacks capacity to handle a sudden increase in patients.
5. Decision-makers will require advice from public health leaders regarding quarantine or other measures to control the spread of an outbreak. There is little experience and few resources available to understand the potential effects of various countermeasures, particularly quarantine.
6. A smallpox outbreak may bring out tensions between federal and state governments, which would have different priorities in response. For instance states may want access to vaccine, control over quarantine measures, and control over their national guard assets. The federal government may want to reserve vaccine for the military or for national outbreak control, to standardize quarantine criteria nationwide, and to federalize the national guard.

Notes from the script of the Dark Winter exercise contain a good summary of federal legislation regarding quarantine [130]. According to Congressman Christopher Shays, commenting on lessons learned from the Dark Winter exercise, “Should a contagious biological weapon be used, containing the spread of disease will present significant ethical, political, cultural, operational, and legal challenges” [131].

What measures would actually be useful for controlling the spread of a localized outbreak and what they would cost society are points that need study and public discussion. People seeking to flee an epidemic could also spread it; control of an outbreak might require forcible restraint of citizens. The need for enforcement of quarantine, if it were medically recommended, would raise difficult issues on how to enforce it, and how to balance the interests of the health of the public versus individual civil liberties [132]. To prevent these decisions from being made rapidly and arbitrarily in a crisis situation, the ramifications of quarantine need to be thought through in advance to provide maximum protection of civil liberties and maximum containment of the epidemic.

Although quarantine has not been invoked for many years, diseases with secondary transmission are not new, and have traditionally been the province of public health. In the United States, CDC has coordinated their control through specific programs for each disease or groups of diseases, such as AIDS, TB, hepatitis, diarrheal diseases, vector-borne diseases and others.

RESPONSE

Effective response to a BT attack requires planning by individual agencies and integration of plans with other agencies and different levels of government. These are described in a chronological manner from detection and surveillance, to outbreak investigation, medical care of ill persons, psychological distress, and preventive treatment to protect the exposed.

Surveillance for Bioterrorism

The longer time lag between release and symptoms is perhaps the most distinguishing feature of biologic agents. With a chemical or nuclear release, casualties are immediate, obvious and may be massive. After the release of a biologic weapon life would go on as normal for several days during the incubation period of the disease before people began to become ill; there would be no disaster scene to respond to. But early detection in this setting becomes of paramount importance because substantial decreases in death or major morbidity may be achieved if medication or vaccination is given soon enough after exposure. One model estimates that if 50,000 persons were infected with anthrax, 5000 deaths would result if preventive therapy were started immediately; whereas 32,875 deaths would result if treatment were started six days after release [133]. The economic consequences would parallel these findings, with an estimated \$14-22 billion saved in medical costs if preventive therapy were started immediately, versus \$320 million to \$1 billion saved if treatment were delayed for six days after the release [134].

Immediate Detection Technology

It would be convenient if technology existed to detect the presence of a bioweapon in the air, water, or food when it was initially released. This would make it easier to apprehend the perpetrator, provide an opportunity to stop the release, and to prevent disease from developing among those who were exposed.

The Defense Advanced Research Projects Agency (DARPA), a research arm of the Department of Defense, is working on methods to detect, diagnose, and treat bioterrorism and other infectious diseases through many ways, including genetic sequencing. One of these research projects is to develop a diagnostic method that would detect disease in an individual before symptoms occur [135].

The Department of the Treasury oversees the U.S. Secret Service, responsible for protecting the President, his family, and other heads of state. The U.S. Secret Service has been developing a biological agent detector and improving its laboratory capacity to detect biological and chemical agents [136].

The Department of Defense has created Civil Support Teams, mobile units capable of testing for the presence of deadly chemicals and biological agents in the field. The teams can be in the field within 4 hours of deployment anywhere in their area of service. From 1999 to 2001, Congress authorized in sequential years 10, then 17 more, and then 5 additional Civil Support Teams. Six teams are cur-

rently certified ready for service. These units are federally funded and trained, but report to the governor of the state they are located in. They are light mobile units. Their mission is to rapidly detect harmful agents in the environment, assess the extent of an incident, and identify measures for decontamination or amelioration [137].

Surveillance Through Monitoring Illness

As environmental detection devices for biological agents are at present mostly in the research stage [unlike devices for the detection of chemical agents], the first sign of a BT attack would likely be illness in victims [138]. In a setting where large numbers of persons are exposed, some persons will develop symptoms earlier than others. These cases, if they are detected early enough, may allow an investigation and response to be initiated in time to protect others who have been placed at risk through exposure [139].

The current systems for monitoring communicable diseases have for years enabled health departments to track trends for the major communicable diseases of public health significance, including TB, syphilis, AIDS, diarrheal diseases, and others. Under these reporting processes, the data are available for analysis several weeks after the onset of illness. Most current systems require a definitive laboratory diagnosis in order to ensure the accuracy of data. Systems require physicians or laboratories to submit data on each case of a reportable illness, frequently done by mailing paper forms to local health departments [140], which are subsequently forwarded through state health departments to CDC. The time delays in these surveillance systems make them inadequate for a bioterrorism incident. There is a need for basic communications infrastructure in public health. A CDC survey of city and county health departments in 1999 found that 20% lacked e-mail capabilities and over half did not have continuous high-speed Internet access [141].

The international capacity to detect outbreaks is even more deficient [142], though progress is underway through the World Health Organization and other groups. ProMED is an international electronic listserv, moderated within the International Society for Infectious Diseases, that posts reports of disease outbreaks among plants, animals or humans [143], and provides a forum for scientific discussion which can assist discovery of outbreaks and their causes. The Infectious Disease Society of America hosts a similar listserv for Infectious Disease physicians and public health practitioners to exchange information [144]. There are also unique isolated projects. An animal disease surveillance project in Africa is underway to monitor and report zoonotic diseases [145].

Syndromic Surveillance

Syndromic surveillance for bioterrorism has been recommended to provide earlier detection of an outbreak [146]. Instead of collecting data about diseases which have been definitively diagnosed, syndromic surveillance monitors the numbers of persons presenting with clusters of symptoms that could be expected

in the very early phases of illness caused by the weaponized BT agents. If there were an effective release of a BT agent, many people would have similar symptoms within a short period of time. Symptom patterns might appear to be non-specific, such as the upper respiratory or gastrointestinal symptoms, which are seen everyday in medical clinics. Such problems are often treated without a definitive diagnosis. But if a larger number of persons than those recorded in past seasons were to become ill with similar symptoms within a short period of time, this increase would only be detected by a system that monitored for such syndromes. At this time, hospitals neither collect nor monitor this sort of data in an ongoing or timely way.

The way hospitals are organized to care for patients provides an example of some of the issues that need to be resolved in order for hospital care to become a good source of BT surveillance data. For rapid information on illness in humans, monitoring hospitals is a logical place to start because hospitals process large numbers of ill persons. Yet hospitals do not report data on communicable diseases in incoming patients. Such reporting is seen as the job of physicians and laboratories after patients have been seen and properly diagnosed, thus assuring accurate data.

An incidental benefit to a syndromic surveillance system is that it could also detect naturally occurring outbreaks. It is likely that outbreaks are being missed under the current system. An example of an outbreak which was missed under current reporting systems but which could have been detected under a syndromic surveillance system is the cryptosporidiosis outbreak in Milwaukee [147]. In this incident, although an estimated 403,000 persons developed transitory diarrheal illness, the outbreak was not detected by public health authorities. The reasons are no surprise to those working in public health communicable disease programs. Most persons probably did not visit a doctor; of those who did few were probably tested; of those tested, cryptosporidium may have been overlooked as it is not usually included in routine laboratory panels for diarrheal illness; and those patients that were tested and appropriately diagnosed may not have been reported to the health department [148]. Health department authorities became alerted to the outbreak because a pharmacist reported his observation that all the over-the-counter anti-diarrheal medications were sold out. This outbreak could have been detected earlier by monitoring data from over-the-counter pharmaceutical sales or by syndromic reporting of the numbers of patients presenting with diarrhea.

In a time when market forces, led by federal reduction of medical payment for Medicare and Medicaid, are forcing hospitals to struggle to stay in business, it is unreasonable to request that hospitals provide additional data to government agencies on the rates of diseases, whether those data are in the form of paper forms or computer reports. Yet effective surveillance would require not only that this be done, but that it be done in a timely and ongoing manner.

One way to do this without taking additional time from hospital staff would be to monitor the streams of data which hospitals generate in the course of patient care (personal communication, M. Williams, St. Louis County Health Department

and T. Bailey, Department of Infectious Diseases, Washington University School of Medicine, 2000). For instance, when chest X-rays are ordered in evaluating patients with respiratory infections [a possible an early sign of some BT agents], monitoring the numbers of chest X-rays ordered per number of patients seen would be a possibility for this sort of monitoring. It could be arranged to identify other computerized data, i.e., the number of prescriptions for antibiotics per number of patients seen that could suggest the early symptoms of a bioterrorism event. If such systems were in place, they could also provide useful information for routine hospital planning, such as for scheduling personnel or ordering supplies. The alerts of potential bioterrorism events generated by this system would need to go to authorities within the hospital or the local health agency which have the responsibility to investigate local outbreaks and take measures to control them. Local authorities would alert state and federal officials if a BT event were suspected.

For a system like this to be effective, many unique agreements would need to be negotiated. Since hospitals are often private entities; it is not possible to negotiate one agreement which would apply to all hospitals. Instead, individual agreements may need to be made with each hospital system. Likewise, hospitals have different data systems so software solutions for reporting may need to be individually tailored to each hospital system. It is possible that standards for electronic medical records would enable the collection of timely syndromic surveillance data without compromising patient confidentiality. If privacy concerns were satisfied, electronic medical record databases could open the door to epidemiologic research and consequent medical advances which have never been possible before.

The Texas Department of Health, in collaboration with CDC and their National Guard (the 6th Civil Support Team), is developing an early detection system based on interpreting electronic data from medical centers in the light of past experience from archival data. They estimate this system would add 24 to 72 hours to their response time through earlier detection of a BT event [150].

Information Sources Needed for Disease Surveillance

A robust surveillance system requires diverse sources of input in addition to hospitals, because early signs of attack could manifest elsewhere. For disease among humans, surveillance should include data sources affected at places where ill people might go. Sales of pharmaceuticals, emergency room visits, hotline phone calls, website visits, emergency medical service calls, urgent care visits, and physician's offices are some of the places to be monitored for increases in the rates of illness that surpass expected rates, based on past experience. Others sources include emergency department utilization, numbers of hospital admissions, Intensive Care Unit occupancy, physician's database searches [151], unexplained deaths, ambulance runs, 911 calls, poison control center calls, and absenteeism in work sites and schools [152].

A BT event might be targeted to cause disease among animals or plants or could do so among animals or plants as an unintended consequence. Therefore

information from agricultural sources, veterinarians, veterinary laboratories, zoos, and departments of wildlife and conservation should be included. Local health agencies would be the appropriate recipient of data on human health; for animals and plants, corresponding data are collected by different governmental agencies.

However, the scope of data sources could potentially be much wider. Because some communicable diseases require certain environmental conditions that are detectable from the air, remote sensing data from satellites could identify times and places where these diseases could exist in the environment, or could monitor for disease in plants. Rose, Huq, and Lipp describe colloquia in which "scientists in the fields of climatology, meteorology, microbiology, medicine, ecology, epidemiology, oceanography, and space science [are collaborating] to study how natural climate variability affects occurrence and prevalence of pathogenic microorganisms, vectors, and disease outcomes" [153]. This interdisciplinary work will require long-term monitoring of disease parameters, including mining archival health data, and will lead to a better understanding of the relationships between our environment and human health. It is possible that surveillance data monitored for climate research could also detect BT events, and it is equally likely that advances in understanding of this field could generate unforeseen possibilities for protection and response.

For each of these sources of information, issues corresponding to those described for hospitals would need to be identified and resolved. Many of the parties which would need to be included in such a system have not viewed themselves a part of a disease surveillance system before: relationships need to be established, legal authority agreed upon between different agencies and levels of government, computer systems designed both to collect and analyze this information, protection of individual privacy ensured, and a mechanism established to feed this information to persons who need to know and with the authority to act on it. It would be reasonable for data from all sources to be monitored centrally. An outbreak among animals can be a sentinel event signaling the risk of an outbreak for humans, as diseases can cross species. Climate and the environment may influence microorganisms in ways we are only beginning to discover. There is a need for greater understanding of these interrelationships. At present, it is not clear what agency would be capable of coordinating and interpreting data from all these resources, or how subsequent investigation and interventions would be arranged. A unit should be designated to integrate disease data from many diverse sources, to begin to interpret their relationships, and to identify early warning signs of a disease outbreak among plants, animals, and humans. This unit will also need a mechanism to initiate investigation and control measures. Some federal funding has been allocated to study this problem among the civilian community. An office within CDC has been designated for bioterrorism surveillance. However, nationally, we are far from a unified, effective system to deal with this complex and critical problem. A high level of authority and priority will be essential to developing an effective surveillance system for communicable disease outbreaks and for bioterrorism.

Outbreak Investigation

One of the charges of public health is to watch over and monitor the rates of disease in the population. At the local, state, and federal levels, authorities follow trends in communicable diseases and look for ways to decrease their incidence. The Centers for Disease Control and Prevention (CDC) is the national agency for public health, working directly with all state health agencies, which in turn provide oversight for local health department programs related to the control of communicable diseases. CDC would provide guidance for the public health investigation and control of a BT outbreak.

When an outbreak is suspected, several processes begin. Case definitions are determined and increased surveillance is started to find as many cases as possible. Every case may add to the cumulative body of evidence eventually pointing to the source of the outbreak. Records of hospitals and emergency rooms may be sought, a national advisory issued, and at times the public may be notified through the news media. Background rates of the disease are determined to see if the situation is indeed a rise above the normal rate. As suspected cases are found, environmental and human samples may be sent for laboratory analysis. As information begins to come in, various hypotheses are generated. Often a questionnaire is designed, specific to the outbreak situation, to standardize interviews of persons and allow for statistical analysis.

It is often possible to prevent further transmission even before the cause of an outbreak has been determined, if a factor or exposure is found to be related to disease. A classic example is the closure of the Broad Street pump, in eighteenth century London, which stopped a cholera outbreak before there was an understanding of microorganisms. The pump was shut down simply because it was noted that persons who obtained their water from that pump had a much higher rate of disease.

Epidemiology is the basic science that gives public health tools for these activities. Epidemiologists are experienced in distinguishing a real increase from apparent increases in rates of disease, in conducting statistical analyses sometimes necessary to do this, in applying the various techniques needed to collect and interpret data, and in the methods to investigate and control outbreaks when they occur. These skills have enabled investigators to track down unknown diseases and find the causes of new outbreaks, like Hanta virus [154].

There is a need for many more trained epidemiologists at all levels of public health [155]. For nearly two decades funding shortages and hiring freezes for communicable disease programs in local and state public health departments have left these departments with skeletal crews with haphazard ability to detect outbreaks [156]. Epidemiologists are a critical defense in detecting all outbreaks, including bioterrorism events. Finding persons with these skills can be difficult. More students of public health specialize in law or management, which offer the possibility of more lucrative jobs in the private sector, than specialize in epidemiology, which requires more science and statistics. Even students specializing in

epidemiology may graduate without training in infectious disease epidemiology or outbreak investigation. The CDC has a two year training program called the Epidemic Intelligence Service (EIS) which enrolls about seventy persons every year. But few health departments can afford to hire these persons at the salaries that graduates of either of these training programs would expect. If funding were available and designated for health departments to hire trained epidemiologists [157], schools of public health might encourage more students to obtain these skills. A trained public health staff nationwide would greatly improve public health response capabilities for detection of all health problems as well as bioterrorism preparation.

Although it is improving, there has been a divergence between the fields of private and public medicine; few physicians are on the faculties of schools of public health, and medical school curricula have tended to teach little about public health. Few physicians have been trained to be epidemiologists. To effectively control disease, better coordination must occur between the medical community (taking care of individual patients), and the public health community (concerned with trends of disease in the population). These two fields would be more effectively integrated if there were more physician epidemiologists who can speak face to face as equals with both groups.

The CDC has been preparing a national BT response training plan, a crisis communications plan, and has been providing assistance to state and local health departments in many areas of BT preparedness. The CDC has created a website with information on the bioterrorism diseases for physicians, public health workers, and the general public [158].

Coordination of Outbreak and Criminal Investigations

In a suspected terrorist event, public health outbreak investigation staff and law enforcement officials will find themselves working side by side. Public health staff may be called upon to submit reports to local police, the state highway patrol, or the FBI. Public health staff need to be familiar with the rules for evidence, to ensure their ability to testify under oath that all evidence or samples have been collected, stored, and examined properly. Likewise, law enforcement personnel are not accustomed to a concurrent need for witnesses to receive prophylactic medication or undergo laboratory testing. They also may not know how to assist in a public health outbreak investigation. These law enforcement personnel need to become familiar with measures to prevent transmission of illness, and the circumstances when various interventions would and would not need to be applied. Government staff working in different services need to learn about each other's work to develop a coordinated approach to outbreak and criminal investigations. There are also a spectra of privacy and dissemination of information issues that have different legal implications for the medical and law enforcement communities, and that need to be addressed.

Some progress has been made. In January 2000 a group of law enforcement and public health officials met to discuss which parts of their work in a BT inves-

tigation could be shared. Their report [159] identifies portions of information from interviews that could be exchanged, and how and when information would flow between agencies and levels of government most smoothly. In addition, they recommended that law enforcement and public health professionals form joint working groups and develop personal relationships, recommendations which are being followed across the nation.

Outbreaks due to BT agents have international implications as well, as the use of a BT agent violates the Biological Toxin and Weapons Convention. Negotiating an additional protocol to this convention that would establish standards for evidence handling and procedures for investigating outbreaks would be useful in handling the international implications resulting from a BT attack [160]. A BT attack would be grounds for retaliation. If it were possible to identify the aggressor through previously negotiated mechanisms, the support of an international court of law would lend credence to the cause of an aggrieved nation or could clear a nation from suspicion.

The FBI is the lead federal agency for the crisis management of a WMD incident. The FBI has established and trained a WMD Coordinator in each of its 56 field offices. The FBI has the ability to coordinate the deployment of a Domestic Emergency Support Team to assist field offices with technical advice in the management of a WMD event. Through four regional meetings with CDC, the FBI is assisting to prioritize the needs of the public health community. The FBI is working with CDC to develop a secure, web-based communication system between CDC and state health departments called Epi-X, which will give health departments access to health related information without compromising law enforcement sensitive information [161].

The FDA's Office of Regulatory Affairs would have responsibility for the investigation of a bioterrorism attack that targets any product regulated by the FDA. It maintains a 24-hour emergency hotline and has established a notification system with the FBI for bioterrorist events [162].

Laboratory

Whether a suspicious outbreak is a bioterrorism event or a naturally occurring outbreak, the need for rapid, accurate diagnosis of the causative agent is essential; laboratories are critical in confirming the presence or absence of a pathogen, in human samples or in the environment. Laboratory analysis can also identify unique characteristics of an organism, making it possible to distinguish between separate outbreaks of the same disease and track how outbreaks are spreading. The scientific expertise of laboratorians is essential, as well as laboratory facilities and equipment, and computerized communication to forward results of testing. Currently there is a shortage of trained microbiologists; in addition, legislation passed in 1998 lowered educational standards, and has increased the potential that BT pathogens could be overlooked, or that lab accidents could occur [163].

Cost cutting in the medical care system has resulted in fewer laboratory tests being conducted for diagnosis and patient care [164]. However, laboratories can only test samples that they receive. Disincentives to ordering clinical tests must be changed so that physicians are encouraged to use more routine laboratory testing as a part of patient care. This is especially important during influenza season, because some of the BT diseases can look like influenza in their early stages.

Most laboratory work for the diagnosis of human diseases is handled by private laboratories. But there are quite a number of rare diseases for which reagents and facilities are only available at CDC. Smallpox, for instance, because it is airborne and highly contagious, requires Biosafety level 4 (BSL4) facilities; CDC is one of the few BSL4 laboratories in the nation. The capabilities of state public health laboratories vary, but clearly a network of laboratories capable of testing for the BT diseases throughout the country would be valuable both for improved response time and for increasing the national capacity to handle large numbers of samples.

Through funding from CDC, this capacity now exists for the diagnosis of most of the BT diseases at state laboratories throughout the country, instead of being located exclusively at federal agency headquarters. However, adding more laboratories, increasing the capability of existing laboratories, and collaboration between food, water, veterinary [165], and private laboratories could increase the national laboratory capacity further. Currently there are few mechanisms for exchange of information between state laboratories, or between private laboratories in the same region or state, an exchange that could facilitate early recognition of an outbreak [166]. Laboratories need BT response plans with measures to handle a massive influx of specimens, packaging of some specimens to higher-level laboratories, and mechanisms to handle increased numbers of inquiries from patients, families, and the news media [167].

The Hazardous Materials Response Unit within the FBI conducts research on laboratory evidence of attribution for biological material. It has also worked with the CDC to develop laboratory protocols that include the chain of custody necessary for a criminal investigation, and to assist the CDC in developing its Laboratory Response Network for bioterrorism [168]. The U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) would provide back up to CDC for confirmation of the diagnosis when identifying bioterrorism agents and would also work with the FBI in a terrorist incident [169].

Mass Medical Care

Hospitals face a host of problems which tend to prevent even their participation in the emergency planning process for BT: among these, decreases in financial revenues [170] and workforce capacity [171], and increases in regulatory demands [172], leave them with few administrative resources for emergency planning. Reductions have occurred in major sources of income for hospitals from Medicare, to Medicaid managed care, and tight private coverage contracts. There

is little financial margin left over for unfunded projects such as emergency planning. Hospitals are facing a growing number of federal regulatory demands: billing system accuracy, safer needles, greater patient privacy, limitations on medical devices, and medical and medication error reduction. Creating industry standards for both WMD preparedness and regional planning could level the playing field by requiring all hospitals to comply. A 2001 Chemical and Biological Institute report [173] recommended that a federal task force be formed to identify the barriers to hospital participation in the BT planning process, and propose some workable solutions. This report also recommended that federal grants should be extended to hospitals for planning and for participation in regional emergency planning.

Skeletal Staffing of Hospitals

Increased competition among hospitals and a constant effort to improve cost efficiency have caused hospitals to trim their staff and facilities till they are operating near to full capacity as often as possible. This has resulted in a national trend towards decreasing surge capacity in hospitals and medical facilities, that is, their ability to expand capacity to meet a sudden need for hospital care. This is unfortunate in the face of an increasing threat for BT, or even an unexpected large natural outbreak. In 1999, a routine Influenza season caused an increase in the volume of patients large enough to deplete the hospital resources in many regional areas, forcing them to close their doors to new patients [174]. Hospitals can prepare to increase their surge capacity by maintaining lists of retired workers and arranging for contingency use of alternate care sites. However a mass casualty bioterrorism event is likely to overwhelm even such enhanced resources very quickly.

An important factor to consider in emergency planning is that the majority of hospital and health care workers are female (many are heads of households), and have responsibilities in the home taking care of family members. If these persons were to continue reporting to work over the relatively long period of time a bioterrorist incident would require, hospitals would need plans for the care of staff family members.

Workforce Shortage in the Medical Field

There are workforce shortages in every area of the health care industry [176], including physicians, nurses, pharmacists, food service workers, housekeepers, and office staff. The shortages are broad in scope and likely to be long term. The same changing demographics which will result in more patients in future years, are also likely to result in fewer health care workers in a profession which has been traditionally dominated by younger individuals. In addition, there has been a change in the image of health care professions as careers; they have been seen as less attractive; and fewer persons are entering the workforce in the health professions.

Need for Infection Control Plans at Hospitals

Hospitals need plans which accommodate the differences in medical care required for various BT agents. The Association for Professionals in Infection Control has created standards for infection control measures, which define specific precautions health care workers should apply in caring for victims of BT agents [177]. Diseases which have the capacity for secondary transmission [the spread of disease from infected persons to individuals not exposed to the initial release] may require measures for isolating large numbers of patients for health care and possibility quarantine for health care personnel and others exposed to these patients. Diseases treated with ventilatory support [178] may require collaboration between hospitals to develop plans for acquiring ventilators, bedspace, and staff to care for these patients. Ideally, specific plans would be delineated for each ward and personnel for each type of emergency. Pre-existing agreements with hotels or like facilities to handle housing of massive numbers of ill or quarantined persons will be needed, along with all the attendant needs of hospital care; such as meals, bedding, and laundry.

The Agency for Healthcare Research and Quality (AHRQ), under the oversight of HHS, supports research designed to improve health care through improved quality and reduced costs, which has included research on ways to improve the preparedness of both health care providers and institutions in response to a bioterrorism attack. Its research projects specific to bioterrorism have included information and decision support systems [179].

Regional Planning

For effective care of mass casualties, it would be optimal to triage patients external to the hospitals receiving them [180]. "Effective triage can reduce system stress by separating the worried well, the potentially exposed, and the sick, and sending them to the appropriate care facility, which may include self-medication in the home" [181]. Triage of patients to different facilities implies regional planning, a rare occurrence in today's competitive health care field, but which will be essential to maximize the limited assets of hospitals [182].

Some regulations, requiring hospitals to treat any ill person who arrives at their facility, do not contain a provision for regions to designate hospitals to receive either "uninfected" or "infected" patients—a measure that could decrease the regional transmission of infectious diseases during an outbreak situation. There needs to be a capability to waive these regulations for emergencies, in order to facilitate pre-hospital triage of patients [183] to prevent patients with communicable diseases from exposing health care workers and other patients to the risk of infection [184].

Planning for the Arrival of Federal Support

Even if federal assets are made available, planning for their arrival will need to be done by staff overwhelmed with many other responsibilities. During the

TOPOFF exercise in Denver, hospitals lacked the staff to keep track of either the numbers of patients they had received or their available bedspace [185]. There was also a lack of coordination in how that information was reported to public health workers [186] who needed to decide where to send federal medical relief workers. Arrangements also needed to be made for the housing, food, and other needs of relief workers. For any large incident, state and local governments may become overwhelmed with the logistical and resource arrangements that will be needed to support federal assets [187].

The Office of Emergency Preparedness (OEP), within HHS, coordinates a national system for medical care called the National Disaster Medical System (NDMS) which includes participation from the Department of Defense (DOD), with the Department of Veterans Affairs (VA), FEMA, state and local governments, and the private sector. This system coordinates all federal supplemental medical care which could be brought to either a local incident involving civilians within the United States, or to military personnel evacuated from foreign sites, whether the cause of illness is from natural disasters or intentional harm. The NDMS system includes specialized teams of medical personnel called Disaster Medical Assistance Teams (DMAT), mobile teams which are self-sustaining for an initial 72 hours to provide specialized assistance to a disaster. Specific teams address mortuary needs, psychological needs, surgical needs, and other needs. These teams can also provide primary care if local facilities become overwhelmed. Four teams called National Medical Response Teams (NMRS) are trained to respond to events involving weapons of mass destruction. The OEP has conducted training exercises to enhance the adaptability of these teams in working with DOD and DOE and in integrating efforts with local personnel in response to emergency events [188].

Mass Distribution of Emergency Medications

The window of opportunity for the administration of treatments, vaccinations, or remedies for the weaponized disease agents of bioterrorism can be as small as within 24 hours of developing symptoms. For that reason everything possible must be planned in advance to streamline the delivery process of pharmaceuticals as efficiently as possible. The creation of a national pharmaceutical stockpile has made planning for mass treatment or prophylaxis much easier. Problems with stockpiling medications are numerous and complex. Medications expire, so it is necessary to have a rotating supply of items, and inventories may be subject to taxation. Because pharmaceutical companies and hospitals keep low inventories and operate on a “just in time” basis, it is likely local supplies of antibiotics would be depleted in days by a large scale BT event [189]. Local jurisdictions should keep a cache of supplies, with state and federal support, to serve until the arrival of the federal supplies [190].

The CDC’s National Pharmaceutical Stockpile Program (NPSP), has negotiated a contract through the VA to solve some of these problems. The pharma-

ceuticals that would be needed for the agents considered to pose the greatest threat have been prioritized, doses and amounts needed have been calculated, rotating supplies have been arranged, and storage facilities designated. The NPSP is solidifying arrangements with each state for receipt of the materiel. Most states involve their health and public safety departments for this task. Each state must coordinate with CDC on plans for reception, make internal plans for transport and security, and coordinate with local jurisdictions [191]. Local jurisdictions are responsible for on site distribution of medication to the public. Guidelines need to be delineated for local communities on standards for receipt of the NPSP, pre-incident training of volunteers, and identification of characteristics recommended for physical distribution sites.

The VA is under contract with CDC to rotate, store, protect, and transport the stockpile. The OEP has made similar contracts with the VA for medical supplies for the four National Medical Response Teams responsible for responding to WMD incidents. The VA assists in training civilian medical personnel who staff the National Disaster Medical System in WMD response. VA hospitals participate in local community emergency planning activities and sometimes deploy to presidentially declared national emergencies [192].

The Food and Drug Administration [FDA] has been working with the CDC on facilitating the safe use of investigational drugs in an emergency setting and safe labeling for pharmaceuticals in the National Pharmaceutical Stockpile Program. Though the task does not fall under its usual responsibilities, the FDA has been compiling a list of medications that would be effective in a bioterrorism attack, along with information on manufacturers, inventories, suppliers, and lead time for producing the drugs [193].

The Department of Commerce, through the Office of Law Enforcement Standards, provides standards and user guides for equipment such as respirators, and decontamination and detection devices used by persons working in criminal justice and public safety to make sure they are safe and effective. This Office also assists DOD and DOJ in preparing a Standardized Equipment list of technical equipment considered essential for responding to terrorist attacks [194].

Prioritization of Vaccine Recipients

Influenza is a vaccine-preventable disease responsible for a large number of deaths every year among the elderly and persons with certain chronic diseases [195]. These persons should have priority to receive the influenza vaccine if there is a delay in the supply, which happened in 2000 [196] and 2001 [197]. Because vaccines are distributed through the private sector which has little incentive to prioritize recipients, in most states there is no mechanism to assure that influenza vaccine gets preferentially to those who need it most. Similarly, a potential issue in the distribution of BT pharmaceuticals is the prioritization of risk groups in the face of limited supplies. Should vaccine or medication be reserved for just those known to be exposed? What about health care workers who encounter ill persons in their work? If a large expanding outbreak is in process, it could be important to

ensure the safety of those who keep power and water supplies functioning, and the safety of fire, police, and emergency workers, the National Guard, the military, and others. These decisions will require hard choices, planning, and forethought.

Handling Mass Mortalities

Mass casualty events from a BT attack would result in new problems, requiring new plans. Bereaved families will have varying requests for disposition of bodies and effects of the deceased. These will have to be balanced with the need for preservation of evidence required to build a legal foundation for subsequent prosecution. For instance, legal requirements may indicate that testing and sampling be documented for each victim—an impossibility in a mass casualty situation where the number of victims greatly overwhelms testing and storage capacity. Cities do not maintain morgue space for large numbers of casualties, so alternative arrangements should be postulated.

Discussions need to occur between hospital staff, medical examiners, and law enforcement so that in a BT event the needs of each discipline can be addressed under constraints of both time and resources. Procedures also need to be in place for handling the personal property of victims, autopsy reports, and samples. Eventually, these discussions may require legislation to clarify procedures for mass casualties.

Death notification should occur as rapidly as possible, and be handled by professionals with training and experience [198]. It could be useful to consolidate the responsibility for notification of family members of the deceased, and associate this task with some provision of bereavement counseling for them, but this is unlikely to happen unless it is planned. Providers of counseling and psychological care for the bereaved need to be identified in advance and plans made for how these arrangements will be activated. The many different agencies offering services and compensation for victims should share information to simplify the paperwork required of victims and to streamline their benefits process [199].

Psychological Distress

Among the persons presenting for care in the wake of a mass casualty event will be persons with symptoms due to psychological causes, some of which can become long term. Six months after the bombing of the Oklahoma City federal building in 1995, 34% of survivors had Post Traumatic Stress Disorder (PTSD), and 23% major depression [200]. The numbers of psychological victims will likely increase according to the intensity of the stress [including the numbers of physical victims, surprise, lack of preparation, tired or deficient leadership, and the inexperience of psychiatric teams]. Many of these features are likely to be present in a BT attack [201]. Distinguishing the physical and psychological victims will be neither trivial nor easy, and some persons may fall into both categories. Symptoms of psychological distress can overlap with the signs of early illness from

many of the BT agents: fatigue, headache, muscle aches, joint pain, and nausea or vomiting [202].

Whatever the cause of the patient's symptoms, pain and distress are real and must be treated. Based on the numbers of psychological casualties in the sarin gas attack in Tokyo, there may be as many as four psychological casualties for every physical casualty in a large mass casualty incident [203]. These psychological victims should be included in disaster planning [204], and provisions made for diagnosis and care for these psychological victims. Five years after the 1995 sarin gas attack in Tokyo, in 2000, out of 191 victims who responded to a survey, many still had lingering psychological effects, including depressed mood (13%), flashback experiences (13%), and physical symptoms such as fatigue (16%), stiff muscles (15%), and headache (10%) [205].

Following the Oklahoma City bombing, it was found that 76% persons who later developed PTSD had shown early symptoms within one day of the bombing, and 94% within one week. In psychological terms, these early symptoms are called "avoidance" and "numbing", and include going out of the way to avoid thinking about the event, an inability to feel love, and a sense of pointlessness in thinking about the future [206]. Although some studies have found that early symptoms have low predictive value for long-term effects [207], systems to look for these symptoms could provide a way for the identification of some persons who could benefit from early intervention. Groups who have been found to be at greater risk for developing PTSD include females, those with concurrent significant physical injuries, and those with major concurrent negative events in their lives [208]. Since it is likely the number of psychiatric casualties will exceed the physical casualties, planning for psychiatric care is essential.

Health care workers and those responding to an event may also become psychological casualties [209] and may be at higher risk than others [210]. Disaster plans should include ongoing measures for monitoring psychological stress among workers and arrangements for persons who need help to receive it in a timely manner, both to prevent worsening of acute symptoms and decrease the risk of subsequent psychological consequences. A program in the Air Force which encouraged staff to seek mental health services if they needed them reduced suicides by 50% [211].

Training and exercise scenarios for emergency responders should include actor victims who have been trained to demonstrate signs of psychiatric distress, and should teach responders in the prevention and mitigation of psychiatric distress [212]. Victims should be broadly defined to include first responders. Victims should be rapidly identified, quickly given access to information and services, sources of funding, and the qualifications of those providing services [213].

Mental health professionals need to be involved in the preparation for response to mass casualty events. Research is needed on the effectiveness of Critical Incident Stress Debriefing, a method of psychiatric intervention which has advocates and doubters among mental health care professionals [214].

The Office of Justice Programs (OJP) in some cases can provide direct assistance to victims of terrorism, such funding for as the provision of mental health treatment. The JTF-CS and the NDMS, previously mentioned, also have psychiatric care units [215]. The Substance Abuse and Mental Health Services Administration (SAMHSA), under the auspices of HHS, is responsible for behavioral health issues [216]. The American Red Cross also offers many services that address psychological needs.

COMMUNICATIONS

Communication Between Responding Agencies

During a BT incident, there will be a need for rapid and accurate communication between responders at local, state, and national levels, between agencies with different functions, and private sector agencies such as hospitals and clinics [217]. The Health Alert Network, a program administered to state and local health departments through CDC, has enabled many local health departments to obtain computers with Internet access, an essential infrastructure for rapid communication necessary for during an infectious disease outbreak. Many agencies are setting up procedures both to operate and to receive notifications at night. The TOPOFF exercise revealed that there is a need for communications equipment to be compatible [currently some responding agencies have communications equipment that operates on limited and non-compatible frequencies], and for redundancy of methods in case some means of communication fail [218].

It would be useful to develop the capacity for online communication connecting all the various agencies responding to an emergency. Such a system would provide, according to the needs of each participating agency: access to information about when and where events occurred, which agencies were involved in the response, what steps were being taken by which agencies, the names of contact persons within organizations, maps, and a mechanism to share other pertinent data. Such a computer system would decrease the confusion in an emergency and enhance the ability of all persons involved to respond promptly and effectively. The system might be tailored to existing emergency response systems already in use, so that each agency would see a screen that looked familiar to them, but that would enhance their system by allowing them access to appropriate parts of the larger developing picture. Confidentiality of data across institutional lines, assurance of appropriate access to this system, computer logistics, and assignments of responsibility for this system are examples of the issues that would need to be resolved.

The Office of Emergency Preparedness, housed within HHS, has conducted both preparedness and research activities. It has also worked on enhancing systems for communication during disasters [219].

Public Information

In a BT incident, the victims would not be the only intended targets of the attack; presumably terrorists intend to instill fear and disrupt society. Because biological weapons are unfamiliar to most people, their use carries additional potential for panic and fear. How the media handles such an event will have critical implications for public reaction. In the midst of enormous public interest, a balance should be sought between providing immediate information and validated, accurate information. If multiple experts give variations in opinion, the public will need an authoritative source for medical information, and a way to correct rumors [220]. As always, balanced accurate media coverage with a sensitivity to context is an art; a BT attack would test the mettle of both reporters and the public.

The media may help the public to assist in controlling the disaster by identifying where and when the release may have occurred, determining who may have been exposed, and relaying information to others regarding interventions such as medications, vaccines, or measures individuals can take to protect themselves from disease. The pivotal role of the media dictates that advance planning of this process should occur to a detailed level to ensure maximum accuracy and efficiency.

A government report on media relations in WMD [221] has recommended that all levels of government engage the media before a crisis, that plans include designating mental health experts with media experience who could convey sound advice to the public in a crisis, that the public be informed about best and worst case scenarios, and what the government is doing to resolve the situation. Other recommendations included identifying "validators", who can provide good information and "credible sources", who are skilled at conveying information to the public, targeting news appropriately for different audiences, and providing methods for two-way communication to correct misinformation, such as hotlines and websites.

FUTURE DIRECTIONS

Training

A part of developing new response procedures is to train those who would need to participate in them. Because bioterrorism is a new threat, many persons who would be called upon to respond may require training about what bioterrorism is, and what the symptoms, diagnosis, and treatment of weaponized agents are, before they are ready to assimilate training on their role in response plans.

Many stand-alone programs have been developed for training, but a longer term approach would institutionalize BT training, as required material, with specific standards for training and recertification of diverse professionals: health care professionals, lawyers, public health professionals, first responders, policy-

makers, research scientists, agricultural workers, veterinarians, and others. Institutionalized training will require defining basic knowledge requirements for each category of professionals so that these can be included in the training curricula for each of these groups [222]. If these components were also to be included in certification requirements for re-licensing, for example, it would be assured that working professionals were updated both currently and on an ongoing basis as this field progresses. A useful report recommending this approach in specific terms has been developed on this subject for those working in the emergency medical system [223]. This approach could allow for re-allocation of money currently being spent in possibly redundant training programs [224].

The Department of Justice (DOJ), through the FBI, is the lead federal agency for crisis management of any terrorist incident in the United States. Its Office of Justice Programs (OJP), has overseen programs to provide first responders with training, equipment, technical assistance, and exercises [225]. Most of the Domestic Preparedness Program previously responsible for these was transferred from the Department of Defense (DOD) to the Department of Justice (DOJ) in October 2000 [226]. This program has several components providing expertise to help train civil emergency responders at the local, state, and federal levels in responding to incidents involving weapons of mass destruction or high-yield explosives. The DOD [227] has worked with OEP on the creation of the Metropolitan Medical Response System (MMRS), described below, and has coordinated yearly tabletop exercises designed to test major components of local response plans. Its Expert Assistance Program includes a WMD helpline to assist in non-emergency planning, a website, a hotline for immediate access to technical expertise during an incident, and a database with information about chemical agents, biological agents, detection devices, and personal protective equipment.

FEMA [228] is the lead federal agency in the managing the consequence phase of a terrorist attack. It supports training at the state and local levels for emergency planners and officials in other agencies with a role in emergency response. It funds grants for state agencies to develop terrorism annexes to existing disaster plans which can be used by states in different ways to fit needs specific to each state, such as training, conducting exercises, or other planning activities. FEMA funds training provided through the Emergency Management Institute and the National Fire Academy, and maintains databases on WMD agents meant to serve as a resource guide for response. FEMA is collaborating with DOD and DOJ on updating the Standardized Equipment List which first responders use in purchasing their supplies. Together with the National Emergency Management Association, FEMA is creating a self-assessment tool for government agencies to detect areas for improvement in their emergency plans. A baseline survey using this tool in 1998 reported areas that states could improve on in their plans and equipment for response to a terrorist incident.

The Metropolitan Medical Response System (MMRS), overseen by the OEP, has trained senior staff in local first response agencies, health agencies, hospitals, and trainers in 120 cities, including providing funding for equipment and other

projects [229]. This program contracts collectively with local agencies that have in many instances not worked together closely in the past, to improve the integration of local plans for response to a WMD incident. The OEP has collaborated with the Institute of Medicine to conduct research on developing assessment and performance measures to improve these MMRS programs nationwide. These programs initially tended to be weighted towards public safety responders: fire, police, and emergency management [230]. The OEP is overseeing a project in Charlotte, North Carolina, in 2001 to enhance the health care system contribution to this process, including community health care systems, medical providers, and the public health system.

Through the Office of State and Local Domestic Preparedness Support, the OJP [231] has provided funding to 120 larger metropolitan areas for emergency equipment and training targeted to the first responder community: fire, emergency medical, and public safety personnel. The Office also conducted a survey to assist local communities in determining their risks and needs and to obtain an overall picture of the comparative preparedness of the metropolitan areas. The OJP has directed one-day exercises in 52 cities, in which personnel from public health, fire, law enforcement, and emergency management agencies worked through a bioterrorist incident from its incubation period through its conclusion, requiring personnel to address quarantine, mass mortalities, medical surveillance, and patient tracking.

The CDC provides oversight for several hospitals and universities engaged in research and training for bioterrorism preparedness [232].

The OEP [233] provides management staff and funding for the U.S. Public Health Service Noble Training Center in Alabama, a center training first responders in responding to a WMD incident. The Center is also developing training materials on WMD response for physicians, nurses, and emergency medical technicians.

Training for the General Public

Training for the general public should be balanced to promote knowledge without creating a sense of fear and should begin prior to a BT attack. Education should raise awareness of the principles of infectious diseases, and the strengths and weaknesses of biological warfare. Public participation is essential in implementing disease control measures for any disease. Dissemination of information to the public in advance has been recommended as an effective way to decrease panic and mitigate psychological stress during a real event as it removes the element of surprise [234, 235]. Understanding the mechanisms of disease transmission and how to protect oneself on an individual level would also alleviate individual personal unease, because it gives direction for action [236]. If people know beforehand that they might need to do nothing in particular for a BT attack except to follow public health recommendations on the news, this could help prevent an atmosphere of panic. Individuals who washed their hands frequently, avoided

crowds, and stayed at home, could possibly decrease the spread of agents with secondary transmission.

There are also opportunities for the public to plan participation in a large disaster: volunteers will be needed to help with the distribution of the NPSP, or could receive training in how to provide basic interventions to psychiatric victims to help prevent later psychiatric effects [237]. Agencies providing services to victims could benefit from working together to recruit, screen, and train volunteers to assist in responding to a BT attack [238].

Research

General Research Needs

The Defense Science Board has recommended creating 1) a database of “signatures” of the biological warfare agents, 2) small diagnostic tools capable of immediately detecting all agents in the database, and 3) a computerized system for alerting defense and public health responders to the possibility of an outbreaks [239]. Scientific collaboration on discovering relationships between climate and human health have been mentioned previously.

There is need for understanding of potential effects of various quarantine measures or mass prophylaxis measures on the control of disease, and their cost in lives and dollars. Study of the quarantine measures should address “implementation authority, enforcement, logistics, financial support, and psychological ramifications” [240]. The more thoroughly these issues are resolved in advance, the safer our civil liberties will be. Research is also needed on the causes for low public trust and how better trust could be restored [241].

In addition to planning and training, many agencies are involved in research projects. The Department of Energy (DOE) [242] houses a Chemical and Biological National Security Program, which conducts research related to bioterrorism as part of a larger mandate to reduce the danger from weapons of mass destruction. It has an analysis component which postulates the value of projected research through simulation models. Its technology development component conducts advanced research on detection methods, modeling capabilities, decontamination procedures, and methods for both attribution and medical countermeasures based on molecular biological studies. Its Domestic Demonstration and Application programs are developing future operational systems based on the integration of existing technology for specific applications.

The Department of Defense has for years been involved in research and treatment of unusual diseases, including tropical infectious diseases and those caused by agents of biological warfare. USAMRIID is the lead institution for these activities [243]. Research projects include developing vaccines, therapeutics, and databases for assistance in diagnostic procedures. The institute is equipped with a Biosafety Level 4 laboratory, one of the few in the world in which researchers can study dangerous airborne pathogens safely. The USAMRIID is

collaborating with the NIH on developing an anthrax vaccine, and also collaborating with other military agencies in developing plans for potential support to civil authorities following a terrorist incident.

The OJP has research programs which collaborate with the FBI, the Technical Support Working Group, and the Office of State and Local Domestic Preparedness Support to determine the agents that terrorists are most likely to use [244].

The Technical Support Working Group is an interagency body chaired by DOD and DOE which has been working since 1987 on accelerating the development of technologies to combat terrorism [245]. The National Institutes of Health (HHS) is composed of 27 separate institutes and centers, and additionally funds research in private facilities nationwide [246]. The FBI, through its Hazardous Materials Response Unit, conducts research on the identification of biological agents directed towards developing capabilities for attribution of an event, to person, group, or geographical region. Some of this research was conducted by the Massachusetts Institute of Technology and some by the U.S. Soldier Biological and Chemical Command [247].

Vaccines

Anthrax vaccine is an example of an effective pharmaceutical that could be used in an outbreak situation to protect persons from exposure or to decrease the length of time exposed persons would need to take protective antibiotics [248]. Production of this vaccine has been delayed because its sole supplier, Bioport, has had difficulties meeting FDA standards [249]. Unfortunately, problems with the supply of anthrax vaccine are not unique. The vaccine industry has had difficulties resulting in shortages of many vaccines [250]: meningitis, tetanus toxoid, yellow fever, and others. Because they don't bring in large revenues, pharmaceutical companies have less incentive to produce vaccines than some of their other products. In view of the lack of economic incentive for their development in the private sector, government oversight and funding for vaccine research and production should be considered. Vaccines could also be potentially powerful tools against BT; another endeavor that would require federal funding.

While a shortage of these vaccines is worrisome in this country, medical care in America is available to unvaccinated persons who become ill, and the presence of a majority of vaccinated persons in communities has a tendency to keep outbreaks from spreading. In the developing world, a lack of vaccines results in much suffering and mortality from preventable causes. Measles, preventable by vaccine, kills nearly one million children each year in the developing world; childhood vaccines that cost just a few cents each could save an estimated 3 million lives a year [251]. There is a need for research and development of new vaccines, both for diseases that cause tremendous mortality worldwide and for the BT diseases. Jack Woodall, the founder of ProMED, has proposed an international transparent scientific collaborative effort to develop vaccines against the BT diseases [253]. Research on vaccines could also decrease the risk of BT by employ-

ing experienced scientists from the dismantled Russian biological weapons program. Furthermore, if research could result in vaccines and other measures for the prevention of infectious diseases that currently plague the developing world, it is possible significant savings in lives could occur, also resulting in strengthened economies and increased political stability.

The subject of global poverty and disease is worth a mention. A recent article in *The Economist* argues that while it may be too glib to attribute the root causes of terrorism to poverty and disease in the developing world, that nevertheless there is likely a correlation between rates of illness in countries and political instability, and that reducing the rate of infectious diseases in the developing world may result in fewer states which could offer safe haven for terrorist groups. The article holds that every country bears responsibility for appropriating their own resources towards some measure of health care for their citizens, yet calculates that even with judicious use of funds, some countries simply do not have enough money. While acknowledging that donated funds are often diverted by corrupt officials, the article suggests that the dire need should motivate wealthier global citizens to persist in trying to help. It calculates that with proper use of funds, if every citizen in the developed world would contribute monies worth approximately less than two tanks of gas for most cars, that “a colossal number of lives could be saved, and immeasurable suffering relieved.” [253]. These are complex issues, but the stakes are high and we cannot afford to ignore them.

The National Institute of Allergy and Infectious Diseases (NIAID) is an NIH institute which houses a program conducting research on diagnostic methods, vaccines, and therapeutic medications for the bioterrorism diseases. Its research has been focused on smallpox, developing early detection methods, extending the shelf life of existing vaccine, preventing complications from the smallpox vaccine, and developing new therapeutic medications for smallpox. It also formed a Working Group on Anthrax Vaccines collaborating with USAMRIID and other agencies to develop and test a new anthrax vaccine [255].

The FDA’s Center for Biologics Evaluation and Research conducts research to ensure both the efficacy and safety of vaccines against the bioterrorism diseases, including anthrax, smallpox, and plague. The FDA’s Center works with CDC and DOD to establish a system of lot numbers and surveillance activities that would detect adverse side effects from vaccines. The FDA’s Center for Devices and Radiological Health has been evaluating for safety a device intended to detect anthrax in humans, and is developing processes for allowing the use of investigational devices such as these in an emergency situation. The FDA’s Center for Drug Evaluation is developing corresponding processes for allowing the use of investigational medications in an emergency situation.

Because many of the bioterrorism diseases do not affect humans naturally, it is often not possible to conduct studies on vaccines, devices, or medications for these diseases using human data as is usually done. In an emergency situation

such as a bioterrorism attack in which no other diagnostic methods or therapy may be available, the use of investigational methods which have not been previously studied in humans, may be the only option to protect exposed persons. To solve this problem, the FDA is working with NIH, CDC, and other agencies to develop standards for the use of animal and laboratory data in licensing diagnostic devices and pharmaceuticals for emergency use in protecting the public from a bioterrorism attack. Since there may be no natural market for these vaccines, medications, and diagnostic devices, this work is dependent on government funding for its research [256].

The CDC also conducts its own research on anthrax, smallpox, and other bioterrorism diseases. The DOT is conducting research on improving metropolitan area responses to WMD incidents in local mass transit systems [257].

Genomics

Because biological agents are living organisms, they have the potential for genetic alteration. Organisms could be genetically altered to be antibiotic or vaccine resistant, have enhanced aerosol and environmental stability [258], elude standard detection and diagnostic methods [259], or evolve into new diseases after therapeutic treatment is administered for their first phase [260]. Genetic modulators could be produced to cause anything from mood changes to altered functioning of the immune system. If this possibility has not been ignored by those in the business of weaponizing biological agents [261], neither are those in this country unaware of how to deal with new diseases. New diseases such as Legionnaires' disease [262] and Hanta virus [263] have been identified in the past and will continue to be identified. Nevertheless, new diseases would impose further difficulties in dealing with a biologic attack. The method of transmission would have to be identified to prevent further spread of disease, a method of laboratory diagnosis would have to be found to identify which persons have been affected by the outbreak, and effective treatments found. However, our advancing understanding of the genomic technologies which have the potential to make biowarfare more deadly, may also provide the hope for new solutions. If an increased understanding of the immune system, and its interactions with genetic modulators resulted in effective and rapid response measures, it could serve as a major deterrent to BT in general. Solutions could enable discoveries in diagnostics and treatments to be so rapid they would "render biological warfare or terrorism an obviously futile as well as morally unacceptable act" [264].

The NIAID, an agency of the NIH, has a large research program conducting research on the genomics of the bioterrorism diseases and how they affect the pathogenesis of disease. Identification of the genomic sequences of the bioterrorism diseases will pave the way for new diagnostic methods and therapeutics for diseases [265].

CONCLUSIONS

Recommendations and ideas for action have been placed throughout the chapter as they fit into each topic of discussion. Rather than a summary of points covered in the chapter, these conclusions suggest trends that may be beneficial in developing defenses against BT, and some perspectives on thinking about the subject.

First, knowledge is key to conquering the threat of BT. The public and those working in all levels of government need to understand the threat of BT and what measures would be effective to protect the population. All components of society [individual agencies; federal, state, and local levels of government; and various disciplines] have unique characteristics, assets, and challenges that will present different opportunities for progress in this multi-faceted field. Widespread knowledge of problems and potential solutions will allow each entity to make progress as their own situation allows.

Many separate and fragmented systems need to become integrated and work together on common goals. The nation's public health system, lacking in basic infrastructures such as electronic communications systems and trained staff, must now forge closer or even new relationships with many entities: the medical community to track disease in humans; the veterinary, wildlife, and agricultural communities to track disease in animals and plants; the intelligence community to track threats and investigate outbreaks; and the public safety and military communities to plan response. Further, ultimate solutions will depend on new advances in genetics, immunology, laboratory science, technology, and epidemiology, and will involve international collaboration. This alignment of purpose throughout government and the private sector is unlikely to occur without informed leadership, entrusted with broad powers. Public support will be critical to create the political will for this integration, which will need to cut some redundant programs in order to fund other areas that are lacking.

The government's electronic communications should reflect these relationships. There is a need for a more integrated infrastructure for the appropriate exchange of information across agency lines, levels of government, the medical and veterinary communities, research institutions, and private industry. This would greatly enhance the ability of the United States both to detect an outbreak and mobilize a coordinated response. This electronic network should be secure, maintain individual and agency confidentiality, and be adaptable. Epidemiologists throughout the process should participate in the interpretation of data so that trends are spotted rapidly.

But the scope of this problem is larger than any one country. As BT programs were started because of international conflict, solutions to the threat they pose must also be international in scope. Negotiation of treaties and conventions will help clarify expectations and standards. International collaboration also needs to deepen in other areas, including law enforcement and scientific exchange. An appreciation for the medical problems in the developing world, with research into

vaccines and other measures to stem the worldwide toll of communicable diseases, would help stabilize the world economy, provide work for underemployed scientists with dangerous skills, and advance the medical knowledge of mankind. Finally, the roots of conflict are often economic. It is possible that if affluent countries can apply some of their resources to alleviating disease and poverty abroad, less of that disease and poverty will be brought back home from other countries, one way or another.

(Acknowledgements: Paul Fennewald, Jefferson City FBI Office, reviewed the manuscript concerning the role of law enforcement in response to a BT event. Thaddeus Zajdowicz, MD, Office of the Joint Task Force for Civil Support reviewed it regarding the role of the military. Eddie Hedrick, Director of Infection Control, University of Missouri Hospitals, Columbia, reviewed it for hospital planning and infection control. Their reviews were very important and very much appreciated. The CDC Health Alert Network and Epi-X updates have been of noteworthy assistance in the scientific and public health areas. The Physicians Online website provided the view of physicians in practice. The weekly electronic Homeland Security newsletter, published by the ANSER Institute for Homeland Security, provided many sources for this chapter. (Some of these sources have not been attributed in the references section to the newsletter through my own filing errors). This on-line journal provides an ongoing, balanced account of issues related to homeland security, describing federal activities and legislation influencing the governmental process, and advances in science and technology, and I highly recommend it for anyone interested in this subject. Finally, the assessments and conclusions are my own and are not to be considered those of the Missouri Department of Health and Senior Services or the University of Missouri, Columbia.)

REFERENCES

1. A Camus. *The Plague*. New York: Vintage Books. a Division of Random House, 1948.
2. FF Cartwright, M D Biddiss. *Disease and History*. New York: Dorset Press, 1972.
3. A Karlin. *Man & Microbes: Disease and Plagues in History and Modern Times*. New York: G.P. Putnam's Sons, 1995.
4. U.S. National Intelligence Council; *The global infectious disease threat and its implications for the United States NIE*, January 2000, p. 46. <<<http://www.odci.gov/nic/>>> accessed 1/14/02.
5. L Garrett. *The Coming Plague, Newly emerging diseases in a world out of balance*. New York: Farrar, Straus & Giroux, 1994.
6. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 221-222.

7. T Mangold, J Goldberg. *Plague Wars, the Terrifying Reality of Biological Warfare*. New York: St. Martin's Press, 1999, pp. 214.
8. GW Christopher, TJ Cieslak, JA Pavlin, EM Eitzen. Biological warfare: A historical perspective. *JAMA* 278(5): 412-417, 1997.
9. EJ DaSilva. Biological warfare, bioterrorism, biodefence and the biological and toxin weapons convention. *EJB Electronic Journal of Biotechnology* 2(3): 1, Dec 15, 1999. <<<http://ejb.ucv.cl/content/>>> accessed 1/14/02.
10. H Gold. *Unit 731 Testimony*. Tokyo: Yen Books, 1996, pp.17.
11. SH Harris. *Factories of Death, Japanese Biological Warfare, 1932-45, and the American Cover-Up*. New York: Routledge, 1994, pp. 152-157.
12. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 24-113.
13. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, p. 86.
14. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, p. 201.
15. T Mangold, J Goldberg. *Plague Wars, the Terrifying Reality of Biological Warfare*. New York: St. Martin's Press, 1999, pp. 41-52.
16. T Mangold, J Goldberg. *Plague Wars, the Terrifying Reality of Biological Warfare*. New York: St. Martin's Press, 1999, pp. 215-282.
17. T Mangold, J Goldberg. *Plague Wars, the Terrifying Reality of Biological Warfare*. New York: St. Martin's Press, 1999, pp. 322-334.
18. M Leitenberg. An assessment of the biological weapons threat to the United States. *J. Homeland Defense* 2000. <<<http://www.homelanddefense.org/journal/Articles/Leitenberg.htm>>> accessed 1/8/01.
19. K Alibek, S Handelman. *Biohazard, The chilling true story of the largest covert biological weapons program in the world –Told from inside by the man who ran It*. New York: Dell Publishing, 1999.
20. J Miller, S Engelberg, W Beard. *GERMS, Biological Weapons and America's Secret War*. New Jersey: Simon & Schuster, 2001, pp. 125.
21. T Mangold, J Goldberg. *Plague Wars, the Terrifying Reality of Biological Warfare*. New York: St. Martin's Press, 1999, pp. 283-321.
22. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 175.

23. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 153.
 24. K Alibek, S Handelman. *Biohazard, The chilling true story of the largest covert biological weapons program in the world –Told from inside by the man who ran It*. New York: Dell Publishing, 1999, pp. 281.
 25. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999.
 26. M Leitenberg. An assessment of the biological weapons threat to the United States. *J. Homeland Defense* pp. 15-16, 2000. <<<http://www.homelanddefense.org/journal/Articles/Leitenberg.htm>>> accessed 1/8/01.
 27. K Alibek, S Handelman. *Biohazard, The chilling true story of the largest covert biological weapons program in the world –Told from inside by the man who ran It*. New York: Dell Publishing, 1999, pp. 18-20.
 28. PJ Boyer. The Ames Strain, How a sick cow in Iowa may have helped to create a lethal bioweapon. *The New Yorker* November 12, 2001, pp. 72.
 29. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 55-57.
 30. K Alibek, S Handelman. *Biohazard, The chilling true story of the largest covert biological weapons program in the world –Told from inside by the man who ran It*. New York: Dell Publishing, 1999, pp. 118.
 31. DR Franz. Presentation on bioterrorism to media representatives sponsored by the Missouri Department of Health and Senior Services and CDC, August 2001
 32. PJ Boyer. The Ames Strain, How a sick cow in Iowa may have helped to create a lethal bioweapon. *The New Yorker*. November 12, 2001, pp. 69-70.
 33. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 152.
 34. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 123.
 35. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 166.
 36. H Gold. *Unit 731 Testimony*. Tokyo: Yen Books, 1996.
 37. Interview with Dr. Ken Alibek. *J Homeland Security* September 28, 2000. *Homeland Security Newsletter*. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 7/13/01.
-

38. MMWR (The Morbidity and Mortality Weekly Report). Biological and Chemical Terrorism: Strategic plan for preparedness and response. 49:RR-4, April 21, pp. 5-6, 2000.
39. DA Henderson. The looming threat of bioterrorism. *Science* 283:1279-1283, Feb. 26, 1999.
40. JB Tucker. *Scourge: The Once and Future-Threat of Smallpox*. Atlantic Monthly Press, 2001.
41. MT Osterholm, J Schwartz. *Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. New York: Delacorte Press, 2000, pp. 17.
42. JB Tucker. *Scourge: The Once and Future Threat of Smallpox*. Atlantic Monthly Press, 2001, pp. 45-122.
43. R Preston. Dept of amplification: updating the small pox vaccine. *The New Yorker*, January 17, pp. 27, 2000.
44. R Preston. The demon in the freezer. *The New Yorker*, July 12, pp. 46, 1999.
45. DR Franz, PB Jahrling, AM Friedlander, DJ McClain, DL Hoover, WR Bryne, JA Pavlin, GW Christopher, EM Eitzen. Clinical recognition and management of patients exposed to biological warfare agents. *JAMA* 278(5):405, August 6, 1997.
46. J Chin. Editor. *Control of Communicable Diseases Manual*. 17th ed. Washington, D.C. American Public Health Association, 2000.
47. USAMRIID (U.S. Army Medical Research Institute of Infectious Diseases). *Medical Management of Biological Casualties Handbook*. 4th Edition. February, 2001.
48. R Zajtchuk. Editor in Chief. *Textbook of Military Medicine. Part I. Medical Aspects of Chemical and Biological Warfare*. Published by Office of the Surgeon General. Department of the Army, USA. 1997, pp. 467-677.
49. DR Franz, PB Jahrling, AM Friedlander, DJ McClain, DL Hoover, WR Bryne, JA Pavlin, GW Christopher, EM Eitzen. Clinical recognition and management of patients exposed to biological warfare agents. *JAMA* 278(5): 399-411, August 6, 1997.
50. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 244.
51. GAO (General Accounting Office). *Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities*. GAO-01-915. September, 2001.
52. MT Osterholm, J Schwartz. *Living terrors, what America needs to know to survive the coming bioterrorist catastrophe*. New York: Delacorte Press, 2000, pp. 158-159.

53. RJ Larsen, RA David. Homeland defense: state of the union. J Homeland Security <<<http://www.homelandsecurity.org/journal/Articles/article/cfm?article=13>>> accessed 6/8/01.
 54. M Dobbs. Homeland security: new challenges for an old responsibility. J Homeland Defense. <<<http://www.homelanddefense.org/journal/Articles/Dobbs.htm>>> accessed 3/19/01.
 55. GAO (General Accounting Office). Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities. GAO-01-915, pp. 41-43. September, 2001.
 56. GAO (General Accounting Office). Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities. GAO-01-915, pp. 45. September, 2001.
 57. Center for Nonproliferation Studies. Monterey Institute of International Studies. Clinical and Biological Weapons Resource Page. <<<http://www.cns.miiis.edu/research/cbw/domestic.htm>>>. accessed 10/12/01.
 58. J Heinrich. Bioterrorism, Coordination and Preparedness. Testimony before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations. Committee on Government Reform. House of Representatives. GAO 02-129T, pp. 21-22.
 59. J Heinrich. Bioterrorism, Coordination and Preparedness. Testimony before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations. Committee on Government Reform. House of Representatives. GAO 02-129T, pp. 7-11.
 60. J Miller, S Engelberg, W Beard. GERMS, Biological Weapons and America's Secret War. New Jersey: Simon & Schuster, 2001, pp. 358.
 61. Second Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. <<<http://www.rand.org/organization/nsrd/terrpanel>>> accessed 1/14/02.
 62. Road Map For National Security: Imperative For Change, Phase III Report Of The United States Commission On National Security In The 21st Century. March 15, 2001. << http://www.homelandsecurity.org/sugg_reading/Phase_III_Report.pdf >> accessed 1/14/02.
 63. RJ Larsen, RA David. Homeland defense: state of the union. J Homeland Security. <<<http://www.homelandsecurity.org/journal/Articles/article/cfm?article=137>>> accessed 6/8/01.
 64. GAO (General Accounting Office). Combating Terrorism, Selected Challenges and Related Recommendations. Report to Congressional Committees. GAO-01-822. September, 2001, pp. 41.
-

65. Executive Order Establishing Office of Homeland Security. October 12, 2001 <<<http://www.whitehouse.gov/news/releases/2001/10/print20011008-2.html>>> accessed 10/12/2001.
66. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 8/03/01.
67. E Smithson, Prepared statement before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services. October 17, 2001, pp. 2.
68. JS Gilmore, III. Hearing of the Committee of Government Affairs. U.S. Senate. Responding to Homeland Threats. Is Our Government Organized for the Challenge? Sept. 21, 2001 <<http://www.senate.gov/~gov_affairs/092101witness.htm>> accessed 09/28/01.
69. GAO (General Accounting Office). Combating Terrorism, Selected Challenges and Related Recommendations. Report to Congressional Committees. GAO-01-822. September, 2001, pp. 14-15.
70. E Smithson. Prepared statement before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services. October 17, 2001, pp. 2.
71. GAO (General Accounting Office). Combating Terrorism. Selected Challenges and Related Recommendations. Report to Congressional Committees. GAO-01-822. September 2001, pp. 131-136.
72. HHS (Health and Human Services). HHS names physician to coordinate anti-bioterrorism initiatives. HHS News. <<<http://www.hhs.gov/news/press/2001pres/20010710a.html>>> accessed 07/16/01.
73. GAO (general Accounting Office). Bioterrorism, Federal Research and Preparedness Activities. Report to Congressional Committees. GAO-01-915. September 2001, pp. 48.
74. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, pp. 196. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 8/03/01.
75. L Garrett. Betrayal of Trust; the Collapse of Global Public Health. New york: Hyperion Books. 2000, pp. 539.

76. L Garrett, The nightmare of bioterrorism: *Foreign Affairs* 80(1): 82, January-February, 2001.
77. Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, U.S Department of State Archives. << <http://www.state.gov/www/global/arms/treaties/bwcl.html> >> accessed 1/14/02
78. M Whelis. Investigating disease outbreaks under a protocol to the biological and toxin weapons convention. *Emerging Infectious Diseases* 6:6, November-December, 2000. <<<http://www.cdc.gov/ncidod/EID/vol6no6/wheelisohtm>>> accessed 11/20/00.
79. FAS Public Interest Report. Controlling biological weapons: it's time for action. *J Federation of American Scientists*. 53(5): 2, 2000. <<<http://www.fas.org/faspir/v53n5.htm>>> accessed 01/02/01.
80. L Garrett. *Betrayal of Trust; the Collapse of Global Public Health*. New York: Hyperion Books, 2000. pp. 498.
81. DR Franz, R Zajtchuk. Biological terrorism: understanding the threat, preparation, and medical response. *Disease-a-Month* 46:2, February 2000.
82. SM Block. The growing threat of biological weapons. *American Scientist* 89(1): pp. 8, January-February, 2001.
83. Biological Weapons Convention, Stop the clock, support the ban. *The Economist* June 14, 2001.
84. SM Block. The growing threat of biological weapons. *American Scientist* 89(1): pp. 9, January-February, 2001.
85. J Miller, S Engelberg, W Beard. *GERMS, Biological Weapons and America's Secret War*. New Jersey: Simon & Schuster, 2001, pp. 317.
86. L Garrett. *Betrayal of Trust; the Collapse of Global Public Health*. New York: Hyperion Books, 2000, pp. 505-507.
87. MT Osterholm, J Schwartz. *Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. New York: Delacorte Press, 2000, pp. 110.
88. B Roberts. Editor. *Hype or Reality? The "New Terrorism" and Mass Casualty Attacks*. Chemical & Biological Arms Control Institute, 2000, pp. 275.
89. L Garrett. *Betrayal of Trust; the Collapse of Global Public Health*. New York: Hyperion Books, 2000, pp. 513.
90. MT Osterholm, J Schwartz. *Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. New York: Delacorte Press, 2000, pp. 111-112.

91. R Lugar. Nunn-Lugar: A tool for the new U.S.-Russian strategic relationship. Carnegie Nonproliferation Conference. Homeland Security Newsletter pp. 4-9, June 2001. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 6/22/01 <<<http://www.usinfo.state.gov/topical/pol/arms/stories/01061901.htm>>> accessed 06/22/01.
92. L Garrett. *Betrayal of Trust; the Collapse of Global Public Health*. New York: Hyperion Books, 2000, pp. 513.
93. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 249.
94. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, pp. 265-267.
95. CDC (Centers for Disease Control and Prevention). CDC Guidelines for handwashing and environmental control. <<http://www.cdc.gov/ncidod/hip/GUIDE/hand_wash_pre.htm>>
96. A Kohnen. Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture. BCSIA Discussion Paper 2000-29. ESDP Discussion Paper ESDP-2000-4. John F. Kennedy School of Government, Harvard University, October 2000. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 10/12/01.
97. HL Hinton. Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. Testimony before the Committee on Governmental Affairs, U.S. Senate. GAO-02-162T, October 17, 2001. pp. 9-10. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 10/19/01.
98. MT Osterholm, J Schwartz. *Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. New York: Delacorte Press, 2000, pp. 75.
99. WHO (World Health Organization). *Health Aspects of Chemical and Biological Weapons: Report of a WHO Group of Consultants*. 1970, pp. 87.
100. E Regis. *The Biology of Doom. The History of America's Secret Germ Warfare Project*. New York: Henry Holt and Company, 1999, pp. 117.
101. GAO (General Accounting Office). *Bioterrorism, Federal Research and Preparedness Activities*. Report to Congressional Committees. September 2001, GAO-01-915, pp. 76-77.
102. RG Luthy. *Safety of our Nation's Water*. Testimony before the U.S. House of Representatives, Committee on Science. Hearing on H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure. November 14, 2001.

103. RG Luthy. Safety of our Nation's Water. Testimony before the U.S. House of Representatives, Committee on Science. Hearing on H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure. November 14, 2001, pp. 4.
 104. RG Luthy. Safety of our Nation's Water. Testimony before the U.S. House of Representatives, Committee on Science. Hearing on H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure. November 14, 2001. pp. 5.
 105. GAO (General Accounting Office). Bioterrorism, Federal Research and Preparedness Activities. Report to Congressional Committees. GAO-01-915. September 2001, pp. 76-77.
 106. TJ Torok, RV Tauxe, RP Wise, JR Livengood, R Sokolow, S Mauvais, KA Birkness, MR Skeels, JM Horan, LR Foster. A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. *JAMA* 278(5): 389-395, August 6, 1997.
 107. GAO (General Accounting Office). Bioterrorism, Federal Research and Preparedness Activities. Report to Congressional Committees. GAO-01-915. September 2001, pp. 58-59.
 108. GAO (General Accounting Office). Bioterrorism, Federal Research and Preparedness Activities. Report to Congressional Committees. GAO-01-915. September 2001, pp. 59-60.
 109. TV Inglesby, DA Henderson, JG Bartlett, MS Ascher, E Eitzen, AM Friedlander, J Hauer, J McDade, MT Osterholm, T O'Toole, G Parker, TM Perl, PK Russell, K Tonat. Anthrax as a biological weapon, medical and public health management. *JAMA*. 281(18): 1735-1745, May 12, 1999.
 110. TV Inglesby, DT Dennis, DA Henderson, JG Bartlett, MS Ascher, E Eitzen, AD Fine, AM Friedlander, J Hauer, JF Koerner, M Layton, J McDade, MT Osterholm, T O'Toole, G Parker, TM Perl, PK Russell, M Schoch-Spana, K Tonat. Consensus statement: Plague as a biological weapon; medical and public health management. *JAMA* 283(17): 2281-2290, May 3, 2000.
 111. DT Dennis, TV Inglesby, DA Henderson, JG Bartlett, MS Ascher, E Eitzen, AD Fine, AM Friedlander, J Hauer, M Layton, SR Lillibridge, JE McDade, MT Osterholm, T O'Toole, G Parker, TM Perl, PK Russell, K Tonat. Consensus Statement: Tularemia as a biological weapon; medical and public health management. *JAMA*, 285:21, pp. 2763-2773, June 6, 2001.
 112. HL Hinton. Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. Testimony before the Committee on Governmental Affairs, U.S. Senate. GAO-02-162T, Oct. 17, 2001, p. 11. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 10/19/01.
-

113. W Allen. West Nile virus is found in St. Louis area, officials say. St. Louis Post-Dispatch, A-section, Oct. 6, 2001.
114. T Mangold, J Goldberg. Plague Wars, the Terrifying Reality of Biological Warfare. St. Martin's Press, 1999, p. 36.
115. E Regis. The Biology of Doom. The History of America's Secret Germ Warfare Project. Henry Holt & Company, 1999. p. 112.
116. L Garrett. The Coming Plague, Newly Emerging Diseases in a World out of Balance. Farrar, Straus & Giroux, 1994, p. 615.
117. E J DaSilva. Biological warfare, bioterrorism, biodefence and the biological and toxin weapons convention, EJB Electronic Journal of Biotechnology; ISSN: 0717-3458; Vol. 2, No.3, Dec 15, 1999, p. 1 <<<http://ejb.ucv.cl/content/vol2/issue3/full/2/2.pdf>>> accessed 1/14/02.
118. University of Georgia, College of Veterinary Medicine, Southeastern Cooperative Wildlife Disease Study Briefs, 17:3, October 2001, p. 3.
119. Kohnen. Responding to the threat of agroterrorism: specific recommendations for the United States Dept. of Agriculture. BCSIA Discussion Paper 2000-29, ESDP Discussion Paper ESDP-2000-04, John F. Kennedy School of Government, Harvard University, Oct. 2000, pp.36-37. Homeland Security Newsletter. <<[http://homelandsecurity.org/bulletin/current bulletin.html](http://homelandsecurity.org/bulletin/current%20bulletin.html)>> accessed 10/12/01.
120. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 36.
121. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 59.
122. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 72.
123. TV Inglesby, DT Dennis, DA Henderson, JG Bartlett, MS Ascher, E Eitzen, AD Fine, AM Friedlander, J Hauer, JF Koerner, M Layton, J McDade, MT Osterholm, T O'Toole, G Parker, TM Perl, PK Russell, M Schoch-Spana, K Tonat Consensus statement: Plague as a biological weapon; medical and public health management. JAMA 283:17, pp. 2281-2290, May 3, 2000.
124. JF English, MY Cundiff, JD Malone, JA Pfeiffer, M Bell, L Steele, JM Miller, Bioterrorism Readiness Plan: a Template for Healthcare Facilities. Association of Professionals in Infection Control [APIC] and the BT Group in the CDC, April 1999, pp. 27-29.
125. DA Henderson, TV Inglesby, JG Bartlett, MS Ascher, E Eitzen, PB Jahrling, J Hauer, M Layton, J McDade, MT Osterholm, T O'Toole, G Parker, T Perl, PK Russell, K To-

- nat. Consensus Statement: Smallpox as a biological weapon; medical and public health management. *JAMA* 281:22, pp. 2127- 2137, June 9, 1999.
126. MMWR. Vaccinia [Smallpox] Vaccine, Recommendations of the Advisory Committee on Immunization Practices [ACIP]. 50: RR-10, June 22, 2001.
127. RE Hoffman, JE Norton. Lessons learned from a full-scale bioterrorism exercise. *Emerging Infectious Diseases*, 6:6, Nov-Dec 2000. <<<http://www.cdc.gov/ncidod/eid/vol6no6/hoffman.html>>> accessed 12/1/00.
128. T O'Toole, T Inglesby. Shining light on Dark Winter, *Biodefense Quarterly*. 3:2, Autumn 2001. <<<http://www.hopkinsbiodefense.org/darkwinter.html>>> accessed 1/7/02.
129. T O'Toole, T Inglesby. Shining light on Dark Winter, *Biodefense Quarterly*. 3:2, Autumn 2001. <<<http://www.hopkinsbiodefense.org/darkwinter.html>>> accessed 1/7/02.
130. Dark Winter Exercise Script << <http://www.hopkins-biodefense.org> >> accessed 1/14/02.
131. Congressman C. Shays. Combating terrorism: In search of strategy, priorities and leadership. National Governors Association Conference, July 2001. *Homeland Security Newsletter*. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 7/20/01.
132. MT Osterholm, J Schwartz. *Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. Delacorte Press, 2000, pp.159-161.
133. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*. The MIT Press, 1998, p.155.
134. AF Kaufman, MI Meltzer, GP Schmid. The economic impact of a bioterrorist attack: are prevention and postattack intervention programs justifiable? *Emerging Infectious Diseases* 3:2, 1-17, April-June 1997, p.12. <<<http://www.cdc.gov/EID/vol3no2/kaufman.htm>>> accessed 8/5/98.
135. GAO Report to Congressional Committees. *Bioterrorism, Federal Research and Preparedness Activities*, Sept 2001, GAO-01-915, pp. 40-41.
136. GAO Report to Congressional Committees. *Bioterrorism, Federal Research and Preparedness Activities*, Sept 2001, GAO-01-915, p. 74.
137. GAO Report to Congressional Committees. *Bioterrorism, Federal Research and Preparedness Activities*, Sept 2001, GAO-01-915, p. 42.
138. *Clinical & Biological Terrorism Research Development to Improve Civilian Medical Response*. National Academy Press, 1999, pp. 65-66. <<<http://books.nap.edu/books/0309061954/html/65.html>>> accessed 1/8/02.
-

139. RA Falkenrath, RD Newman, BA Thayer. America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack. The MIT Press, 1998, p.154.
140. P Quinlisk. Testimony before the subcommittee on national security, veterans affairs, and international relations, committee on government reform, U.S. House of Representatives. July 23, 2001. <<http://www.house.gov/reform/ns/107th_testimony/council_of_state_and_territorial.htm>> accessed 7/27/01.
141. SG Stolberg, J Miller. Bioterror role an uneasy fit for disease centers. N.Y.Times, Nov. 11, 2001, front page.
142. L Garrett. The Coming Plague, Newly Emerging Diseases in a World out of Balance. Farrar, Straus & Giroux, 1994, pp. 592-620.
143. ProMED website: <<<http://www.isid.org/isid/index.html>>> accessed 6/29/01.
144. Emerging Infectious Diseases website: <<<http://www.idsociety.org/EIN/TOC.htm>>> accessed 1/7/02.
145. Preslar. Animal disease surveillance project: recent advances. J. Federation of American Scientists. 53:5, Sept-Oct 2000, p. 15.
146. Smithson, Prepared statement before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services, Oct. 17, 2001, p. 5.
147. WR MacKenzie, NJ Hoxie, ME Proctor, MS Gradus, KA Blair, DE Peterson, JJ Kazmierczak, DG Addiss, KR Fox, JB Rose, JP Davis. A massive outbreak in Milwaukee of cryptosporidium infection transmitted through the public water supply. New England Journal of Medicine 331:3, July 21, 1994.
148. GAO Report to the Chairman, Committee on Agriculture, Nutrition, and Forestry, U.S. Senate. Food Safety: CDC is working to address limitations in several of its foodborne disease surveillance systems. GAO-01-973. Sept. 2001, p.7. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 10/12/01.
149. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, pp. 40-42. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/30/01.
150. L Gaunt, SE Kornguth. The University of Texas Biological and Chemical Countermeasures Program. J Homeland Security, Sept. 21, 2001. <<http://www.homeland_security.org/journal/SciTech/univtexas.cfm>> accessed 9/21/01.

151. V Jormanainen, J Jousimaa, I Kunnamo, P Ruutu. Physicians' database searches as a tool for early detection of epidemics. *Emerging Infectious Diseases*, 7:3, May – June, 2001, pp. 474-476.
 152. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, pp. 37-39, <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/30/01.
 153. JB Rose, A Hug, EK Lipp. Health, climate and infectious disease: a global perspective. *American Academy of Microbiology*, 2001, p. 1. <<<http://www.asmsa.org/acasrc/pdfs/climate2.pdf>>> accessed 1/7/02.
 154. L Garrett. *The Coming Plague, Newly Emerging Diseases in a World out of Balance*. Farrar, Straus & Giroux, 1994, pp. 528-549.
 155. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute, 2001, pp. 61-64. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
 156. L Garrett. *The Coming Plague, Newly Emerging Diseases in a World out of Balance*. Farrar, Straus & Giroux, 1994, p. 605.
 157. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, p. 64, <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
 158. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 53.
 159. NDPO/DOD, Criminal and epidemiological investigation report. Held on January 19-21, 2000. DTIC SBCCOM Biological Wartime Improved Response Program, Dec. 2000.
 160. M Whelis. Investigating disease outbreaks under a protocol to the biological and toxin weapons convention. *Emerging Infectious Diseases* 6:6, Nov-Dec 2000. <<<http://www.cdc.gov/ncidod/EID/vol6no6/wheelisoh.htm>>> accessed 11/20/00.
 161. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 70-71.
 162. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 60.
-

163. JW Snyder, W Check. Bioterrorism threats to our future; the role of the clinical microbiology laboratory in detection, identification, and confirmation of biological agents. American Academy of Microbiology and the American College of Microbiology, p. 11. Homeland Security Newsletter. <<http://www.homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/17/01.
164. JW Snyder, W Check. Bioterrorism threats to our future; the role of the clinical microbiology laboratory in detection, identification, and confirmation of biological agents, American Academy of Microbiology and the American College of Microbiology, p. 6. Homeland Security Newsletter. <<http://www.homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/17/01.
165. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute, 2001, p. 78. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
166. JW Snyder, W Check. Bioterrorism threats to our future; the role of the clinical microbiology laboratory in detection, identification, and confirmation of biological agents, American Academy of Microbiology and the American College of Microbiology, 2001, p. 6. Homeland Security Newsletter. <<http://www.homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/17/01.
167. JW Snyder, W Check. Bioterrorism threats to our future; the role of the clinical microbiology laboratory in detection, identification, and confirmation of biological agents, American Academy of Microbiology and the American College of Microbiology, 2001, p. 5. Homeland Security Newsletter. <<http://www.homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/17/01.
168. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 70.
169. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 43.
170. R Pollack. Commentary – Facing the fragility of health in America. Health Forum, June 2000 <<<http://www.healthforum.com/HFPubs/asp/ArticleDisplay.asp?PubID=&ArticleID=15828&Keyword=Work>>> accessed 1/7/02.
171. Workforce Supply for Hospitals and Health Systems: Issues and Recommendations Developed by the AHA Strategic Policy Planning Committee – Approved as a Statement of interim positions by the AHA Board of Trustees, January 23, 2001. American Hospital Association. <<http://www.aha.org/workforce/advocacy/Workforce_B0123.asp>> accessed 1/7/02.
172. Patients or Paperwork: The Regulatory Burden Facing America's Hospitals. American Hospital Association. <<<http://www.aha.org/ar/Advocacy/paperworkreport/asp>>> accessed 1/7/02.

173. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, p. 174. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
 174. E. Smithson. Prepared statement before the Senate Committee on Governmental Affairs, Subcommittee on International Security, Proliferation and Federal Services, Oct. 17, 2001, p. 6.
 175. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, p. 101. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
 176. JD Bentley. Challenges for hospitals, strategic policy planning, American Hospital Association. Presentation at The 2nd National Symposium on Medical and Public Health Response to Bioterrorism: Public Health Emergency & National Security Threat, Nov 28-29, 2000.
 177. JF English, MY Cundiff, JD Malone, JA Pfeiffer, M Bell, L Steele, JM Miller, Bioterrorism Readiness Plan: a Template for Healthcare Facilities, Association of Professionals in Infection Control [APIC] and the BT Group in the CDC, April 1999.
 178. SS Arnon, R Schechter, TV Inglesby, DA Henderson, JG Bartlett, MS Ascher, E Eitzen, AD Fine, J Hauer, M Layton, S Lillibridge, MT Osterholm T O'Toole, G Parker, TM Perl, PK Russell, DL Swerdlow, K Tonat. Botulinum toxin as a biological weapon, medical and public health management. JAMA 285:8, February 28, 2001, pp.1059 – 1070.
 179. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 48.
 180. A Mass Casualty Care Strategy for Biological Terrorism Incidents, Neighborhood Emergency Help Center. Prepared in response to the Nunn-Lugar-Domenici Domestic Preparedness Program by the Department of Defense, May 1, 2001. <<http://www2.sbcom.army.mil/hld/downloads/bwirp/nehc_green_book.pdf>> accessed 1/7/02.
 181. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute, 2001, p. xvi. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
-

182. AE Smithson, LA Levy. Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response. The Henry L. Stimson Center, Report No. 35, October 2000, p. 309 <<<http://www.stimson.org/>>> accessed 1/8/02.
183. E Smithson. Prepared statement before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services Oct. 17, 2001, p. 6.
184. L Hinton. Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. Testimony before the Committee on Governmental Affairs, U.S. Senate. GAO-02-162T, Oct. 17, 2001, p. 11. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 10/19/01.
185. GAO. Testimony before the Committee on Veterans' Affairs, House of Representatives. Homeland Security. Need to consider VA's role in strengthening federal preparedness. GAO-02-145T, October 15, 2001, p. 8. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 10/19/01.
186. RE Hoffman, JE Norton. Lessons learned from a full-scale bioterrorism exercise. Emerging Infectious Diseases, 6:6, Nov-Dec 2000, p. 2. <<<http://www.cdc.gov/ncidod/eid/vol6no6/hoffman.htm>>> accessed 12/1/00.
187. L Hinton. Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. Testimony before the Committee on Governmental Affairs, U.S. Senate. GAO-02-162T, Oct. 17, 2001. pp. 9-10. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 10/19/01.
188. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 62-66.
189. MT Osterholm, J Schwartz. Living Terrors, What America Needs to Know to Survive the Coming Bioterrorist Catastrophe. Delacorte Press, 2000, pp. 130-131.
190. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, pp. 109-110. <<<http://www.cbaci.org/>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homeland_security.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
191. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 53-54.
192. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 75.
193. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 57-58

194. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 38.
 195. MMWR. Prevention and control of influenza, 50/No Rr-04, April 20, 2001. <<<http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5004al.htm>>> accessed 1/7/02.
 196. MMWR. Updated recommendations from the advisory committee on immunization practices in response to delays in supply of influenza vaccine for the 2000-01 season, 49[39];888-892, Oct 6, 2000. <<<http://www.cdc.gov/mmwr/preview/mmwrhtml/mm4939a3.htm>>> accessed 1/7/02.
 197. MMWR. Delayed influenza vaccine availability for 2001-02 season and supplemental recommendations of the advisory committee on immunization practices, 50[27];582-5, July 13, 2001. <<<http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5027a3.htm>>> accessed 1/7/02.
 198. U.S. Dept. of Justice, Office of Justice Programs, Office for Victims of Crime. Responding to Terrorism Victims: Oklahoma City and Beyond. Oct 2000, NCJ 183949, p. 31.
 199. U.S. Dept. of Justice, Office of Justice Programs, Office for Victims of Crime. Responding to Terrorism Victims: Oklahoma City and Beyond. Oct 2000, NCJ 183949, p. 32.
 200. CS North. The course of post-traumatic stress disorder after the Oklahoma City bombing. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, p. 51.
 201. S Noy. Prevalence of psychological, somatic, and conduct, casualties in war. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 31-32.
 202. RH Pastel. Collective behaviors: mass panic and outbreaks of multiple unexplained symptoms. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp 44-45.
 203. JA Romano, JM King. Psychological casualties resulting from chemical and biological weapons. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 21-22.
 204. EJ Lord. Exercises involving an act of biological or chemical terrorism: what are the psychological consequences? International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 34-35.
-

205. N Kawana, S Ishimatsu, K Kanda. Psycho-physiological effects of the terrorist sarin attack on the Tokyo subway system. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 23-26
206. CS North. The Course of Post-traumatic Stress Disorder. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 51-52.
207. Clinical & Biological Terrorism Research and Development to Improve Civilian Medical Response. National Academy Press, 1999, p. 166.
208. CS North. The Course of Post-traumatic Stress Disorder. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 51-52.
209. Clinical & Biological Terrorism Research and Development to Improve Civilian Medical Response. National Academy Press, 1999, p. 168.
210. Human Behavior and WMD Crisis/Risk Communication Workshop – Final Report. Co-sponsored by Defense Threat Reduction Agency, Federal Bureau of Investigation, U.S. Joint Forces Command. March 2001, p. 27. Homeland Security Newsletter. <<[http://homelandsecurity.org/bulletin/current bulletin.htm](http://homelandsecurity.org/bulletin/current%20bulletin.htm)>> accessed 7/20/01.
211. Human Behavior and WMD Crisis/Risk Communication Workshop – Final Report. Co-sponsored by Defense Threat Reduction Agency, Federal Bureau of Investigation, U.S. Joint Forces Command. March 2001, p. 34. Homeland Security Newsletter. <<[http://homelandsecurity.org/bulletin/current bulletin.htm](http://homelandsecurity.org/bulletin/current%20bulletin.htm)>> accessed 7/20/01.
212. C Di Giovanni. Pertinent psychological issues in the immediate management of a weapons of mass destruction event. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 59-60.
213. U.S. Dept. of Justice, Office of Justice Programs, Office for Victims of Crime. Responding to Terrorism Victims: Oklahoma City and Beyond. Oct 2000, NCJ 183949, p. 30.
214. Clinical & Biological Terrorism, Research and Development to Improve Civilian Medical Response. National Academy Press, 1999, p. 168.
215. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 69.
216. U.S. Department of Health & Human Services, Disaster Mental Health, Substance Abuse and Mental Health Services Administration: The Center for Mental Health

- Services. <<<http://www.mentalhealth.org/cmhs/EmergencyServices/default.asp>>> accessed 1/7/02.
217. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute. 2001, pp. 135-142, <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
218. GAO. Testimony before the Committee on Veterans' Affairs, House of Representatives. Homeland Security. Need to consider VA's role in strengthening federal preparedness. GAO-02-145T, October 15, 2001, p. 11. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 10/19/01.
219. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 62-66.
220. C Quigley. Dual-edged sword: dealing with the media before, during, and after a weapon of mass destruction event. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 56-58.
221. Human Behavior and WMD Crisis/Risk Communication Workshop – Final Report. Co-sponsored by Defense Threat Reduction Agency, Federal Bureau of Investigation, U.S. Joint Forces Command. March 2001. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.html>> accessed 7/20/01.
222. B Roberts. Hype or Reality? The “New Terrorism” and Mass Casualty Attacks. Chemical & Biological Arms Control Institute, 2000, pp. 260.
223. Developing Objectives, Content and Competencies for the Training of Emergency Medical Technicians, Emergency Physicians, and Emergency Nurses to Care for Casualties Resulting from Nuclear, Biological, or Chemical Incidents, Final Report, April 2001. Office of Emergency Preparedness and American College of Emergency Physicians. JHS July 2001.
224. E Smithson. Prepared statement before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services Oct. 17, 2001, pp. 4-5.
225. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 67-68.
226. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 45.
227. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 39-45.
-

228. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 78-80.
229. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 65-66.
230. M Moodie, J Ban, C Manzi, MJ Powers, J Jaworski, S Kishinchand, R Wyman. Bioterrorism in the United States: Threat, Preparedness, and Response. Chemical and Biological Arms Control Institute, 2001, pp. 160-161. <<<http://www.cbaci.org>>> accessed 1/08/02. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 8/3/01.
231. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 67-69.
232. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 49.
233. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 62.
234. S Noy. Prevalence of Psychological, somatic and conduct casualties in war. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 31-32.
235. Human Behavior and WMD Crisis/Risk Communication Workshop – Final Report. Co-sponsored by Defense Threat Reduction Agency, Federal Bureau of Investigation, U.S. Joint Forces Command. March 2001, pp. 49-50. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 7/20/01.
236. M Dobbs. A renaissance for U.S. civil defense? J. Homeland Security, July 2001, p. 6. <<http://www.homelandsecurity.org/journal/Articles/Dobbs_July01.html>> accessed 7/06/01.
237. JP Revel. Meeting psychological needs after Chernobyl: the Red Cross experience. International Conference on the Operational Impact of Psychological Casualties from Weapons of Mass Destruction – Proceedings. July 25-27, 2000. Military Medicine, Suppl. 166:12, Dec. 2001, pp. 19-20.
238. U.S. Dept. of Justice, Office of Justice Programs, Office for Victims of Crime. Responding to Terrorism Victims: Oklahoma City and Beyond. Oct. 2000, NCJ 183949, p. 33.
239. Protecting the Homeland, Report of the Defense Science Board, 2000 Summer Study Executive Summary. Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. Vol.1, pp.13-14. Homeland Security Newsletter. <<http://homelandsecurity.org/bulletin/current_bulletin.htm>> accessed 5/18/01.

240. L Hinton. Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. Testimony before the Committee on Governmental Affairs, U.S. Senate. GAO-02-162T, Oct. 17, 2001, p. 11. Homeland Security Newsletter. <<[http://homelandsecurity.org/bulletin/current bulletin.htm](http://homelandsecurity.org/bulletin/current%20bulletin.htm)>> accessed 10/19/01.
 241. Human Behavior and WMD Crisis/Risk Communication Workshop – Final Report. Co-sponsored by Defense Threat Reduction Agency, Federal Bureau of Investigation, U.S. Joint Forces Command. March 2001, p. 14. Homeland Security Newsletter. <<[http://homelandsecurity.org/bulletin/current bulletin.htm](http://homelandsecurity.org/bulletin/current%20bulletin.htm)>> accessed 7/20/01.
 242. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 46-47.
 243. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 42-43.
 244. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 68.
 245. RA Falkenrath, RD Newman, BA Thayer. America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack. The MIT Press, 1998, p. 312.
 246. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 60-62.
 247. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 70.
 248. MMWR. Use of Anthrax Vaccine in the United States. Recommendations of the Advisory Committee on Immunization Practices. 49:RR-15, December 15, 2000, p. 14.
 249. The growing threat of biological weapons. American Scientist, Jan. 4, 2001, pp. 6-7. <<<http://www.sigmaxi.org/amsci/articles/olarticles/bloclpl.html>>> accessed 01/04/01.
 250. J Woodall. The vaccines for peace proposal, motivating the production of vaccines against dual-threat agents. Sabin Vaccine Report IV-2, Fall 2001, p. 6.
 251. S Flanders. In the shadow of AIDS, a world of other problems. The New York Times June 24, 2001.
 252. Poverty and sickness; terrorism is not the only scourge. The Economist. 351:8253, Dec. 22, 2001, p. 10.
 253. Woodall. The vaccines for peace proposal, motivating the production of vaccines against dual-threat agents. Sabin Vaccine Report IV-2, Fall 2001, p. 6.
 254. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 61-62.
-

255. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 54-58.
256. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, pp. 56-57.
257. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 72.
258. T Mangold, J Goldberg. Plague Wars, the Terrifying Reality of Biological Warfare. St. Martin's Press, 1999, p. 373.
259. B Roberts. Hype or Reality? The "New Terrorism" and Mass Casualty Attacks. Chemical & Biological Arms Control Institute, 2000, p. 196.
260. Inside the Soviet Union's Biowarfare Program: Interviews with Dr. Ken Alibek and Dr. Sergei Popov. J. Homeland Security Journal. 01:01, June 2001, pp. 22-24.
261. J Miller, S Engelberg, W Beard. GERMS, Biological Weapons and America's Secret War. Simon & Schuster, 2001, p. 310.
262. MMWR. Legionnaires Disease- United States. 26:[1997]:300. <<<http://www.cdc.gov/mmwr/PDF/wk/mm4603.pdf>>> accessed 1/7/03.
263. Garrett. The Coming Plague, Newly Emerging Diseases in a World out of Balance. Farrar, Straus & Giroux, 1994, pp. 528-549.
264. CM Fraser, MR Dando. Genomics and future biological weapons: the need for preventive action by the biomedical community. Published online Oct. 22, 2001. DOI: 10.1038/ng.763. p. 17.
265. GAO Report to Congressional Committees. Bioterrorism, Federal Research and Preparedness Activities, Sept 2001, GAO-01-915, p. 61.

11

Nuclear Terrorism: Nature of Radiation

William H. Miller

University of Missouri, Columbia, Missouri

INTRODUCTION

When defining ionizing radiation, one might consider four important factors:

1. How much – what amount of radioactivity is present?
2. How far will the radiation travel – what kind of containment or shield will stop the radiation?
3. How will it affect me – what is the dose from this radiation to the human body?
4. How long will it be around – what is the radioactive half-life?

AMOUNT OF RADIOACTIVITY

Radioactivity is a measure of the rate at which radioactive nuclei disintegrate. It is simply a matter of counting how many of them have decayed, emitting their radioactive particles or waves, in a given amount of time.

As with all measurements, we have a plethora of qualities to define the amount of radioactivity. And, as with many of our measuring systems, we have both “traditional” units and new SI units (International System of Units). The original units are referenced to the Curie (Ci), named in honor of Madam Curie. A Curie is 3.7×10^{10} (37 billion) radioactive disintegrations per second, or approximately the radioactivity of a gram of radium, one of the naturally radioactive elements with which Madam Curie did her research. For many applications of radia-

tion in medicine or industry, the Curie is a relatively large quantity, and so the units of mCi (1/1000th) and μ Ci (1/1,000,000th) are utilized. On the other hand, a nuclear reactor contains millions of Curies of radioactivity and units of kCi (1000) and MCi (1,000,000) are sometimes used. Although the unit of the Curie is being supplemented with the newer SI unit, it is still very much in common use.

The "new" SI unit of the Becquerel (Bq) is named after Henri Becquerel, the discoverer of radioactivity. It is defined as only 1 disintegration per second. Thus it is much, much smaller than the Ci. Multiples of Becquerels are the kBq (1000), MBq (1,000,000), etc. These units are summarized in Table 11.1 below.

Table 11.1 Various units of radioactivity.

Curies	Becquerels or Disintegrations/sec
1 MCi	3.7×10^{16}
1 kCi	3.7×10^{13}
1 Ci	3.7×10^{10}
1 mCi	3.7×10^7
1 μ Ci	3.7×10^4

Becquerels or Disintegrations/sec	Curies
1 Bq	2.7×10^{-11}
1 kBq	2.7×10^{-8}
1 MBq	2.7×10^{-5}
1 GBq	0.027

RADIATION SHIELDING

To understand radiation shielding, it is necessary to differentiate between radioactive material and radioactive particles or emissions. Radioactive material is any material which contains some number of radioactive nuclei. Thus, radioactive materials can be anything, and in fact everything is radioactive to some small degree due to naturally occurring radioactivity in our environment. When the radio-

active nuclei decay, they give off particles or waves that fly out of the nucleus and away from the radioactive material.

To contain the radioactive material, one must simply put it in a vessel that will hold the material and not let it escape. On the other hand, shielding the radioactive particles or waves that they emit is a different matter and depends upon the type of emission. For particles that have a charge on them (like beta or alpha particles), the concept of range is used. The range is the distance beyond which a charged particle cannot penetrate. For example less than 1 cm of plastic is needed to stop all beta particles emitted from a typical radioactive material. For uncharged particles (neutrons) or electromagnetic radiation (gamma-rays or X-rays) the concept of half-value layer (HVL) is used. The HVL is the thickness of shield needed to stop one-half of the radiation that is trying to pass through it. A second HVL stops one-half of what is left, one-half of one-half, or one-fourth of the radiation, etc. A centimeter of lead will stop about one-half of the gamma-rays at a typically energy of 1 MeV emitted from a radioactive material.

The task of containing radioactive material and radioactive emissions is thus a two-step process: 1) containing the radioactive material so that it is not distributed around the environment and 2) stopping the radioactive emissions they give off.

RADIATION DOSE

Radiation exposure and dose define the effect of radioactive emissions (particles or electromagnetic radiation) when they leave the substance containing radioactive nuclei and are then absorbed by the material that receives the dose. Although an engineer might be concerned about the dose to the metal in the reactor vessel in a nuclear power plant, most often we define dose to tissue, e.g., the human body. This dose can then be related to the possibility of adverse effects.

Once again there are numerous units to define this quantity. The older units are the Roentgen (radiation exposure measured as charge deposited per unit volume of air), the rad (radiation dose measured in energy absorbed per unit mass) and the rem (Roentgen equivalent man, or equivalent dose to tissue, depending upon the type of radiation involved). Technically they all have precise scientific definitions, but for most cases are all approximately equivalent. Thus a Roentgen of radiation is approximately equivalent to a rad of dose which is usually equal to a rem of equivalent dose. These units are relatively large compared to typical dose from natural background radiation or even the additional doses experienced by workers in a nuclear power plant or radiologists in a hospital. Again the use of "milli-" is used, i.e., mR, or mrad or mrem, designating 1/1000 as much.

The new SI units are the Grey (Gy) and Sievert (Sv) which are both 100 times larger than the rad or rem, respectively. This is all summarized in Table 11.2.

Table 11.2 Radiation dose.

Exposure	Dose	Dose Equivalent
1 Roentgen	~ 1 Rad	~ 1 Rem*
	~ 0.01 Gy	~ 0.01 Sv*

*Usually an equality, depending upon type of radiation

RADIOACTIVE HALF-LIFE

One interesting feature of radioactive material is that it becomes smaller and smaller as time goes by. Due to the fact that it is decaying, it is self-destructing, and becoming less over time. The rate at which this occurs is defined as the half-life, or the amount of time that it takes for one-half of the radiation to decay. Unfortunately, two half-lives do not eliminate it (i.e. one-half decaying and then the second one-half decaying), but rather the half-life is always referring to how much is left NOW. Thus, one-half life reduces the radioactivity by one-half; two half-lives by one-half of one-half or one-fourth; three half-lives by one-eighth; etc. Thus, radioactivity is never zero, but continues to get diminishingly small as time passes. Radioactive nuclei have half-lives that range from fractions of a second to billions of years. The radioactive material introduced into the body for a medical diagnostic procedure might have a half-life of a few hours so that it decays away to negligible levels in a day or so. At the other extreme, some of the naturally radioactive nuclei in our environment have half-lives of billions of years. The reason that they are still around is that they haven't had enough time to decay to negligible levels since the earth was formed.

SUMMARY

In summary, we have the following definitions:

Radioactivity – how much of it is there?

Curie – 3.7×10^{10} radioactive decays per second

Becquerel – 1 radioactive decay per second

Shielding – how far will the radiation travel?

Range – maximum penetration distance for charged particles

Half Value Layer – amount of material that will stop one-half of uncharged radiation

Dose – how will it affect me?

Roentgen – a measure of the charge created in a volume of air by radiation

Rad – a measure of the energy deposited per unit mass or dose

Rem – Roentgen equivalent man, equivalent dose depending upon type of radiation

Gray – 100 rads; also 1 Joule of deposited energy per kilogram of material

Sievert – 100 rems, equivalent dose

Radioactive Half-life – how long will it be around?

Half-life – the amount of time for one-half of the radioactivity to decay away

RADIOACTIVITY AND RADIATION

The term “radiation” means many different things. Sunlight, the heat from a fire, radio waves, radar, microwave ovens, and radiation emitted from nuclear phenomena are all forms of radiation. These are separated into two types: ionizing radiation and non-ionizing radiation. The radiation emitted from the decay of unstable nuclei is of the former type, i.e., ionizing radiation. Simply put, ionizing radiation has sufficient energy to separate an orbital electron from an atom. Non-ionizing radiation does not. On the scale of electromagnetic radiation, non-ionizing radiation covers the energy spectrum from low energy waves of sonar and short wave radio through medium energy wave of microwaves and radar and up through the energy of visible waves. Above that, electromagnetic radiation achieves enough energy to cause ionizations. This type of radiation is the subject of this chapter.

All nuclei are made up of combinations of protons and neutrons. For most of the lighter elements there is a one-to-one ratio of neutrons to protons (i.e., helium with 2 neutrons and 2 protons), carbon with 6 and 6, sulfur with 16 and 16). As elements get heavier and heavier, the neutron to proton ratio increases to about 1.5 to 1 (i.e., uranium with 146 neutrons and 92 protons). In general, when these ratios are maintained, the nucleus is stable, non-radioactive, and emits no radiation. For some nuclei, however, the nucleus was created with a ratio that is unstable (i.e., uranium-238, potassium-40, and other naturally occurring radioisotopes). Other nuclei have their ratio altered by radiation coming in from outer space (hydrogen 3 or tritium, carbon-14, and other cosmogenic isotopes). Finally, nuclei are altered by human activities like the fissioning of nuclear fuel resulting in isotopes such as strontium-90, iodine-135 and many, many others. Radioactive decay is simply the attempt of a nucleus to move from a proton-to-neutron ratio that is unstable to a proton to neutron ratio that is stable.

To obtain this stable ratio, radioactive nuclei emit particles. The common ones are beta particles (electrons emitted from the nucleus), positrons (positively charged electrons) and alpha particles (a helium nucleus). Beta particles are emit-

ted from nuclei that have too many neutrons to be stable, positrons from nuclei that have too many protons and alpha particles from heavy, unstable nuclei. After emitting one of these particles, the resulting nucleus is a new element that is usually left with an excess amount of energy. This excess energy is emitted as electromagnetic radiation called gamma-rays. Another common form of electromagnetic radiation is X-rays, which emanate from the orbital electrons of an atom that are transitioning from one energy level to another. The other common radioactive particle is the neutron which is largely the product of nuclear fission inside a working nuclear reactor and is not commonly emitted by radioactive materials.

12

Nuclear Terrorism: Radiation Detection

William H. Miller

University of Missouri, Columbia, Missouri

HISTORY OF RADIATION DETECTION

Our bodies have not been designed to detect ionizing radiation, either from particles or electromagnetic waves. Our senses are sensitive only to a narrow band of the electromagnetic spectrum – visible light in a non-ionizing radiation band – and ionizing radiation is more energetic at higher wavelengths. Although radiation is easy to detect with appropriate instruments and at very, very low levels, the human body is unable to detect even lethal doses of radiation.

When radioactive substances were first discovered, the harmful effects of large amounts of radiation were not known and detection instrumentation was not considered. Many scientists who studied radioactivity were exposed to harmful amounts. When X-rays began to be used by doctors, many reported that patients who were exposed to X-rays suffered burns. In 1896, the physicist Elihu Thompson deliberately exposed his finger to X-rays so that he could accurately report on the phenomenon of X-ray burns. Thomas Edison was experimenting with X-rays in 1896 when one of his assistants became fatally ill from over-exposure to radiation. In 1906, Henri Becquerel, the discoverer of radioactivity, was accidentally burned by a radioactive substance he was carrying in his pocket. When Pierre Curie heard of Becquerel's injury, he taped a radioactive substance to his own arm to observe the injuries it would cause.

Henri Becquerel discovered a method of detecting radiation as far back as 1896. He found that the invisible electromagnetic rays and particles from ionizing radiation would affect silver emulsions in photographic plates just like light rays

would. As a result, photographic film has often been used to measure radioactivity.

Film is used for medical X-ray images and for film badges used for measuring personnel dose. The use of X-rays and film to diagnose a broken bone or look for a tumor is familiar to most. For personnel dose measurement, a person who might be exposed to radiation wears a film badge that contains a small bit of photographic film. It is referred to as a dosimeter. The film is covered by a layer of materials such as paper or plastic that prevents light from reaching the film but allows the radiation to pass through. After use, the film is slipped out of the dosimeter and developed. The extent of darkening on the developed film can be translated into a measure of the total amount of radiation received by the person wearing the dosimeter.

Another of the first systems to be used to detect the charge created by ionizations is the scintillation counter. In a scintillation detector the energy of the charged particles created by ionizations excites the scintillator molecules. As they de-excite they emit this radiation in the visible spectrum. The simplest system thus uses the eye to detect flashes of light from the scintillator in a darkened room. Today, photocathodes and photomultipliers are used to electronically detect these light pulses and record them in appropriate counters and spectrometers. A variation on the scintillation detector is liquid scintillation counting, where the sample (usually in the form of a liquid) is introduced directly into the vials containing the liquid scintillation media. Thus the radioactive nuclei and their emissions are in direct contact with the detection medium. This is particularly useful for detecting very small amounts of weakly penetrating radiation.

The task of manually counting scintillation flashes visually was often the task of graduate students, and Geiger was one such student of Rutherford's. Seeking an automated way to detect radiation he helped develop the Geiger-Mueller (GM) tube.

DETECTOR SYSTEMS

Ionizing radiation, by definition, has the capability of knocking off electrons from atoms. Many detector systems allow us to detect this radiation by detecting the charge of these electrons.

In the GM counter, an electric potential is set up between a cylindrical detector wall and a center electrode passing through the center of the cylinder. A gas is used as the detection medium in this cylinder and the negatively charged electrons that are released by ionizing radiation in the gas are collected on the center electrode. This creates an electronic pulse that can easily be detected by a relatively simple electronic circuit. The simplicity of this system, its low cost (as little as a few hundred dollars) and reliability have made it the most utilized radiation monitoring system.

The GM counter is also the basis for a family of gas-filled detectors that work on basically the same principle. These include ionization chambers (free air chambers, Bragg-Gray chambers, pocket ionization chamber), proportional counters (P-10 gas chambers, 2-pi windowless detectors, fission chambers, BF_3 filled detectors), and GM based detectors (cylindrical chambers, pancake probes, end-window tubes).

Since the development of gas-filled detectors and scintillation detectors, a variety of new detection media have been developed for specific applications. A family of solid-state detectors are used for spectroscopy (i.e., determining the energy of radiation). Intrinsic (high purity) germanium detectors are used almost exclusively for gamma-ray spectroscopy. These systems are much more expensive than gas-filled or scintillation detectors, but provide very high energy resolution gamma-ray spectra. The output from these detectors can allow simultaneous quantification of 25 or more radioactive isotopes. Other solid-state detectors include diodes for alpha and beta charged particle detection. These diodes are usually small, coin-sized detectors. Newer solid state materials include CdTe, CdZnTe, HgI_2 , and diamond.

Other miscellaneous detectors include neutron detectors, which are variations on many of the systems mentioned above. They incorporate isotopes which strongly interact with neutrons (such as boron-10, lithium-6, helium-3, uranium-235) in the detection medium. Thermoluminescent dosimeters are used as personnel monitors, performing the same function as film badges. These are small chips of compounds (LiF:Mg , $\text{CaSO}_4\text{:Mn}$, CaF_2 and $\text{CaF}_2\text{:Mn}$) that store the energy of radiation as they absorb it. This energy is released as light when the chip is heated, giving a measure of the sum of radiation absorbed.

Detector Systems in Response to Nuclear Terrorism

To respond to potential terrorist activities involving radioactive materials, first responders should have a basic, portable, hand-held, battery-operated survey meter. This survey meter should include several different probes (detector types) for different functions. First, a standard survey GM tube would be used for general background radiation levels. A GM pancake probe would be important to assess contamination on surfaces or on "swipes" (a piece of paper a few square centimeters in size that is rubbed over a contaminated surface to remove and detect loose contamination). An alpha probe would be included to detect alpha radiation since the G.M. detectors are sensitive only to gamma-rays and beta particles.

Air monitoring to detect airborne radioactive particles would be accomplished using a particulate filter and some sort of air pump. By passing potentially contaminated air through the filter, radioactive particles are captured which are subsequently detected with the GM pancake probe mentioned above. Thus, a basic survey meter would be sufficient to alert first-responders to potentially dangerous levels of external radiation and to radioactive contamination, as well as to airborne radioactive material that could lead to internal radiation doses. This information

would be essential to keep citizens away from radiation areas and to give emergency workers general guidance on their ability to work in the area without receiving dangerous amounts of radiation dose.

Other systems for first responders include self-alarming personnel dosimeters. These are based upon either GM or ionization chambers and include electronic circuitry to alarm when an individual is entering a high radiation level. They are often capable of recording total dose and some include a pancake-type module for surface contamination or swipe counting.

Beyond this simple system, more sophisticated instrumentation should be available at regional universities, nuclear power plants, hospitals, etc. These systems would help to more precisely determine the types of radioactive contamination, quantify the radioactive isotopes involved, and detect radioactivity at lower levels for cleanup efforts. This instrumentation should include high resolution, gamma-ray spectroscopy systems, liquid scintillation counters and charged particle spectrometers.

Beyond the regional level, the federal government can provide assistance with National Laboratory personnel through the Radiological Assessment Program. Similarly, the Federal Radiological Monitoring and Assessment Center can respond with teams of individuals. Both programs include complete analytical instrumentation, sophisticated radiation detection equipment including all of the systems mentioned above, aircraft-based air monitoring systems, and mitigation and clean-up support.

13

Nuclear Terrorism: Dose and Biological Effects

William H. Miller

University of Missouri, Columbia, Missouri

Robert Lindsay

University of Western Cape, Cape Town, South Africa

RADIATION DOSE – NATURAL AND MANMADE

Everything in the world is radioactive to some extent, and always has been. The ocean, the land, the air and our food all expose us to small amounts of natural background radiation. This is because unstable isotopes that give off or emit ionizing radiation are found everywhere. Our exposure comes from terrestrial elements such as potassium, thorium, uranium and radium. In addition, much of the Earth's natural background radiation is in the form of gamma radiation that comes from outer space.

Radiation amounts differ according to one's location on the Earth. Different places on earth have different amounts of rocks and minerals such as uranium, just like we find deposits of coal, copper or lead in different locations. In the U.S. some of the best known deposits of uranium are found in New Mexico, Utah, Wyoming and Colorado. In some parts of India and Brazil there are also high amounts of background radiation from their rocks and minerals. In these places in India and Brazil, the radiation dose rate exceeds the safety limit that the U.S. government has set as the maximum limit outside of nuclear power plants.

A person living in Kerala, India, receives about 1,300 mrems of natural background radiation each year. In the U.S., Colorado has one of the higher averages of about 500 mrems per year. Living near a granite rock formation can increase the background by as much as 100 mrems per year to an individual.

Many different building materials, such as bricks, wood and stone also emit natural background radiation. People living in brick homes are exposed to between 50 and 100 additional mrems per year and in wooden homes between 30 and 50 mrems yearly. Cosmic rays from outer space are another large contributor of natural background radiation. Many of the cosmic rays are filtered out by the atmosphere. At higher elevations there is less atmosphere shielding the radiation coming in from outer space. Generally, exposure increases by about 1 mrem per year for every 100 feet increase in elevation, which is another cause for the higher radiation levels in a state like Colorado. An airplane trip across the U.S. will expose a person to about 2 mrems of radiation because of the high altitude.

Natural background radiation is also found in plants, animals and people. Living things are made of radioactive elements such as isotopes of carbon and potassium. We get about 25 mrems of radiation from the food and water we eat and drink each year. Our bodies harbor more than 5×10^{20} radioactive atoms. About one-half of the radioactivity is in the form of potassium-40, a naturally radioactive form of potassium. Most of the rest of our bodies radioactivity comes from carbon-14 and tritium (hydrogen-3).

Still more radiation is received from manmade sources, primarily from the medical sources for the diagnosis and treatment of disease. We also get small amounts from coal and nuclear power plants and from the residuals of nuclear weapons testing in the 1950s.

Overall, the average person in the U.S. receives 360 mrems per year from all sources, 300 mrems from natural sources and 60 mrems from manmade. The natural dose includes 200+ mrems per year from radon, 40 from internal sources, 26 from space, and 28 from the ground. Manmade radiation includes 40 mrems per year from medical X-rays, 14 from nuclear medicine procedures, and the rest from consumer products, nuclear power plants and other industrial sources.

BIOLOGICAL EFFECTS OF RADIATION

The effect of radiation on humans has been studied in great detail in order to set exposure limits for radiation workers. The survivors and victims of the two nuclear explosions in Japan during 1945 as well as victims of the Chernobyl and other nuclear accidents have been carefully studied. Expert groups (ICRP, BEIR) and the biological results of the exposures have been extensively documented [1]. The cancer treatment programs have gathered further information where the planned damage to malignant cells as well as the unwanted radiation to healthy tissue is carefully monitored [2].

The result of high doses of radiation is fairly clear and well understood but the effect of low levels of radiation is still controversial and leads to much speculation and reporting in the media. Most regulations are based on conservative extrapolation from the results of high exposures.

The biological effects of radiation can be better understood by differentiating between

- i) deterministic effects which can be directly linked to the dose and
- ii) non-deterministic or stochastic effects.

It also helps to distinguish between immediate and delayed effects.

Nuclear radiation is often called ionizing radiation, since it can eject electrons from atoms, a process called ionization. The damage to ONE atom is usually not important, even if it effects the DNA of a cell, since the body is capable of repairing damage on this scale and also has a great deal of redundancy. The earlier discussion shows that humans have been exposed to a certain amount of natural radiation throughout history. This certainly shows that the body is not oversensitive to low amounts of radiation. Health physicist have studied and documented the sensitivity of different organs to radiation but these details are unlikely to be important in a terrorist attack where the exposure is likely to be external.

Immediate (or Acute) Effects

The immediate effects of high doses of radiation are clear. An exposure of about 3-4 Gy during a short period will be fatal within 60 days to 50% of those exposed, the so-called LD50/60-day dose. In cases of exposure above 7 Gy (700 rad) very little can be done for victims. Note that such a dose can only be obtained from:

- i) a nuclear chain reaction in a nuclear explosion
- ii) exposure to the core of a nuclear reactor
- iii) high level radioactive waste or
- iv) the exposure due to extremely strong radioactive sources for an extended period.

The unlikely occurrence of i) and the detailed plans to avoid ii) and iii) have been stressed in other parts of this book.

Acute effects are due to the immediate effect of the deposition of a large amount of energy into the body. The exposure of 4 Gray corresponds to a radiation level where a considerable fraction of the atoms in tissue are affected.

Any value significantly above 5 Gy will be likely to cause death in a very short time. On the other hand, values lower than 0.15 Gray have no easily measurable immediate effect. These two values of about 0.15 and 5 Gy form the lower limit below which there is likely to be no immediate effect and the limit above which nothing can be done to prevent death. Doses between these two values have effects on the blood that can be seen by analyzing the blood.

Apart from the victims who were killed by the blast, most of the fatalities due to the nuclear bombs in Japan resulted from this extreme damage caused to the bone marrow. This led to many deaths during the period a few days to a few

months after the detonation. Victims of more recent nuclear accidents, such as the exposure to a large neutron flux in Japan during 2000, also caused the death of two victims after several weeks a fate that was expected when the doses to which they had been exposed became known. A dose of 2 Gy or higher results in marrow depression which may take a month or two to reach its lowest value, which will take several weeks to be restored, while a 4 Gy dose or higher will often cause irreversible damage followed by death. For doses lower than 2 Gy, the effect will depend on the individual and the exposure level. The effect on bone marrow is a good example of a deterministic effect there is a direct link between the exposure and the depression of the blood count.

Delayed Effects

The delayed carcinogenic effects due to a radiation dose of 1Gy and above are well studied. The onset of cancer is by no means certain, but the probability of the development of tumors is considerably higher than in the case of the rest of the population. For example, the probability of developing leukemia among the Japanese survivors has been about 5 times higher than in the unexposed population. The exposure to radiation leads to cancer by the formation of free radicals that are formed when radiation dissociates water molecules. This can lead to the production of hydrogen peroxide, which is a very powerful oxidation agent. In ways that are not well understood, this can lead to the formation of tumors. The probability of this happening is presumably directly proportional to the radiation dose – at least this is the conservative assumption that is made when dose limits are set. Clearly this effect is different from the acute effects where bone marrow is badly affected by a high dose, but the damage can be repaired by the body unless the dose is too big. Cancer that appears 5-10 years after an overexposure is a stochastic (random) effect. There is not even a way of proving that the cancer is a result of the exposure.

The delayed effects of radiation along with the fact that it may be impossible for people to know the extent to which they have been exposed, will lead to probably the most important health effect of low-level exposure, namely extreme psychological trauma. Any terrorist attack involving radiation will be extremely effective in causing panic.

Even in cases where measurements were available to show that the exposures were low, such as at the Three Mile Island nuclear accident, the emotional effect on the public was severe. No amount of reassuring publicity is likely to counter the general fear associated with radiation.

The above discussion of the effects of an exposure must be understood in the context of the ways in which a dose of 5 Gy can be achieved. Also remember that exposure due to a localized source will fall off according to the inverse square law hence if the exposure level is at a lethal 5 Gray within a distance of 5m from an event, the value 0.15 Gray will be the exposure at about 25 m. Any shielding between the source and the victim, such as buildings, will reduce the dose consid-

erably. Consider, e.g., the exposure due to the sources that are used for the treatment of cancer patients in hospitals or the sterilization of medical instruments. Possible scenarios where such a source is left in a public place have been studied. These sources are extremely strong often in the 10^{14} Bq range. A person spending one minute at a distance of 1 m from such a source will receive a dose of about 0.5 Gy. This would be a very serious exposure that would be regarded as a major accident in the Health Physics field, but it would not cause immediate death. Any other scenario where such a source is dispersed in public will cause a major contamination problem but not lead to any immediate deaths probably not the effect that a terrorist group will want to achieve except for perhaps the psychological effect on the public.

RADIATION DETECTION

Ionizing radiation (along with many chemical and biological agents) cannot be detected with our five senses. However, it can be easily measured with relatively simple instruments at extremely low levels of radiation, levels far below those which would cause harmful effects.

Two examples put the sensitivity of radiation detectors into perspective. First, when one considers the sound of the "click" that a simple radiation detector makes when a single radioactive particle is detected, that click represents the decay of one radioactive nucleus. Thus, the presence of one atom has been detected. In the arena of chemistry or biology, minimum detectable limits by comparison are typically on the order of billions of atoms or molecules. A second example is to consider that a lethal dose of radiation (5 Gy) would correspond to the internalization of over 10^{14} radioactive nuclei which would have to decay in a short period of time to deliver this dose. Radiation detectors are capable of detection one of these radioactive nuclei, and thus the sensitivity is 100 million million times greater than a lethal dose.

Radiation detectors are based upon the fundamental of ionization. In a gas-filled detector, ionization of the gas leads to free electrons that are collected by an electric field and registered by simple electronic counting systems. The Geiger-Mueller tube is of this variety and is the most common detector in use today. These detector systems are available in portable configurations for a few hundred dollars.

In scintillation detectors, the ionization of atoms and the freeing of electrons leads to the production of a small flash of light that can be recorded by a photomultiplier tube and associated electronics. For analytical measurements, solid state detectors such as intrinsic germanium are in common use. These systems are capable of not only measuring the quantity of radiation, but also identifying the radioactive element from which they came. These systems are capable of quantifying as many as 20 to 30 individual radioactive species in a single sample with sensitivities at the parts per million to parts per billion level.

Credible Terrorist Threats Involving Radiation

The National Council on Radiation Protection and Measurements (NCRP) Report No. 138 (2001), "Management of Terrorist Events Involving Radioactive Material" provides critical insights into credible terrorist threats. This report provides a consensus of existing and proposed recommendations from federal agencies and scientific bodies and was drafted by an expert committee of NCRP scientists, consulting federal and state officials.

Based upon the study of the effects of the nuclear blasts in Japan in World War II and having examined the effects of subsequent nuclear weapons testing and the accidental release of radiation from disasters such as Chernobyl, a strong body of knowledge exists about radiation effects and how to minimize them. Short of the use of a nuclear weapon, the spread, or threat of a spread, of some amount of radioactive material probably will cause public concern far in excess of the actual or potential damage to a community or its people.

NCRP Report No. 138 suggests that a terrorist organization is more likely to release a small amount of radioactivity, possibly with an explosion, than it is to obtain and use a nuclear weapon. With the release of small amounts of radioactive material, the necessary containment and cleanup may be well within the capability of public agencies. Such an event could be "catastrophic but manageable."

"When an explosive device is used to disperse radioactive materials, the paradigm shifts. Treatment of casualties is more difficult because of the contamination and the complications associated with other trauma. . . . The debris from the event and other normally harmless materials will be contaminated. The affected area may be much larger than the immediate scene of the crime. The radiological threat, invisible and uncertain in terms of long-term health impacts, will engender considerable public fear and concern.

"At the most basic level is the fact that one of terrorism's chief aims is psychological: to induce fear in a population. Such fear is further compounded when 'invisible toxins,' such as radiation are involved. People can neither see nor sense the presence of radiation, but they know that it is potentially hazardous.

"It must be noted emphatically that radioactive contamination (whether internal or external) is never immediately life threatening and therefore, a radiological assessment or decontamination should never take precedence over significant medical conditions."

For limited releases of radioactive material, people in the area can reduce their exposure by taking shelter in homes or other buildings for hours or a few days until the radiation levels fall. Ventilation systems using outside air should be

shut off and eating contaminated foods should be avoided. Radioactive dust can be washed off of the skin and contaminated clothing should be abandoned to reduce external exposures.

The report places emphasis on the need for public authorities and for scientists to be attentive to the psychosocial effects of terrorism involving the dispersal of radioactive material.

REFERENCES

1. C Herman. Health Physics, 3rd Edition, McGraw-Hill, New York (1996).
2. TD Jones. Proceedings of the thirty-second annual meeting of the national council on radiation protection and measurements: proceedings no. 18: Implications of new data on radiation cancer risk. Health Phys. 73(5), 838-839, (1997).

14

Nuclear Terrorism: Nuclear Weapons

Sudarshan K. Loyalka

University of Missouri, Columbia, Missouri

INTRODUCTION

Nuclear weapons are the ultimate means of destruction, and humanity can ill afford acquisition of such weapons by terrorists. These weapons are a recent phenomenon, but they have spread widely among nations. There are legitimate fears that terrorists could acquire or build such weapons. In this chapter we briefly review the history of such weapons, their effects, and the fundamental technology.

HISTORY

Neutron was discovered in 1932. The following years witnessed intense studies of its properties and interactions with matter. This neutral particle, about 2000 times the mass of an electron, is scattered and absorbed by different materials, with the nature and rate of reaction determined by the nuclei of the host material and the energy of the neutron. Neutrons can also split (fission) some nuclei (the fissile isotopes such as Th-233, U-235, Pu-239), and release energy in the process as kinetic energy of the fission products and beta, gamma and other radiation. New neutrons (2 to 3 on average) are also released in fission, thus providing the basis for a chain reaction. This chain reaction can be sustained (each successive generation has the same number of neutrons), or multiplied (each successive generation has more neutrons), and it can be used for explosive release of energy. Fission of 1 Kg of U-235 or Pu-239 releases an energy equivalent to that obtained in an explosion of about 20 kT of TNT.

WWII imperatives led to the Manhattan Project in the U.S., and construction, testing and use of first nuclear weapons in 1945. These detonations were as follows:

- Test: July 16, 1945, Trinity (NM), Pu-239, 5 kg, 19 kT of TNT
Implosion, efficiency=19%
- Combat Use: August 6, 1945 (Hiroshima). U-235, 49 kg, 17 kT of TNT
Gun (1000ft/sec), efficiency=2%, Known as "Little Boy"
- August 9, 1945 (Nagasaki), Pu-239, 5 kg, 20 kT of TNT
Implosion, efficiency=20% , Known as "Fat Man"

There has been no other combat use of nuclear weapons, but there have been many other detonations, both above ground and underground. The fission bombs have been surpassed with vastly more powerful (~50MT, 1 MT=1000kT) hydrogen or thermonuclear bombs where a fission bomb is used to create a fusion reaction. The announced detonations since 1946 include:

- U.S. (Fission: 1946, 48, 51-62, 63-underground;
Thermonuclear: 10/31/52, Eniwetok, 10.4 MT; 2/28/54, Bikini, 15 MT)
5/20/56, Bikini, Several MT)
- U.S.S.R. (Fission: 8/29/49, Thermonuclear 8/12/53, many other tests)
- U.K. (10/3/52 - Fission and Thermonuclear)
- France (2/13/60 - Fission and Thermonuclear)
- China (1964 - Fission and Thermonuclear)
- India (1974, May 1998, Fission and possibly Thermonuclear)
- Pakistan (May 1998, Fission, U-235 gun type)

It is also widely accepted that Israel has produced and stockpiled nuclear weapons and that South Africa had also produced nuclear weapons and perhaps detonated one. Many other nations have pursued nuclear weapons technology clandestinely at one time or another, and several of them are currently pursuing it.

Nuclear weapons are comparatively compact, and these can be delivered by airplanes, missiles, ships, barges or even trucks. There is speculation that suitcase size nuclear weapons exist.

EFFECTS

A 1/2 ton (TNT) explosive damages an area in about 150 ft radius (e.g., explosion near the Mullah Building in Oklahoma City, or near the U.S. Embassy in Nairobi). By contrast a 20 kT nuclear explosive annihilates an area (people, animals, structures) in a 2 mile radius. A 20 MT thermonuclear bomb can annihilate

an area in a 10 mile radius. Volcanic eruptions and asteroids can have still larger impacts. Suspected asteroid impact 62.5 million years ago was perhaps about 100,000 MT, and it may have led to dinosaur extinction.

In a nuclear explosion, the weapon material and surrounding air (and the suspended soil and other material if it were to be a surface or near surface explosion) reach an extremely high temperature of millions of degrees almost instantaneously. This results in large thermal radiation (as distinct from ionizing radiation) and consequent immediate thermal burns on the living, and fires. The thermal radiation travels at the speed of light, it is absorbed/attenuated by structures, clothing etc. but its effect is felt almost instantaneously. This is followed by shock waves (in a matter of few seconds) and immediate (within a minute) and delayed (after a minute) effects of ionizing radiation discussed in Chapters 11-13. For example, at Hiroshima and Nagasaki approximately 50% of the damage was by the blast and shock, about 35% by the thermal radiation, and the remainder was by radiation, both immediate and delayed. The effect of the shock (pressure/compression) was more significant on structures, while radiation was more damaging to the living.

The effects of nuclear explosions will vary depending upon the height at which an explosion occurs, the weather conditions, the terrain, the structural details (distribution of buildings, the materials they are made of), the population (the age and gender distribution) and the time of the day (whether people are outdoors or indoors, and the clothing they wear).

Use of a thermonuclear weapon for terrorism purposes is unthinkable. First, one requires a fission bomb to trigger a thermonuclear explosion, and second a fission bomb can in itself wreak so much havoc that no terrorists would need to go beyond acquisition of fission bombs for any purpose they might have. A fission bomb is really an ultimate weapon in war, and certainly an ultimate in terror.

WEAPONS TECHNOLOGY

The nuclear weapons technology was born in wartime, and many practical aspects of it have been since well guarded (classified) not only by the U.S. but by other nations also. Many Manhattan Project documents, and the subsequent nuclear literature, however, provide considerable insights into the basic technology.

Each fission of U-235 or Pu-239 releases about 190Mev of energy. Thus approximately 1.5×10^{23} fissions (that is fissioning of about 50 gm of U-235 or Pu-239) are required to produce a 1 kT TNT explosion. A larger explosion will require that many more fissions. These fissions must be achieved while the weapon is still intact, as the expansion (explosion) leads to a rapid cessation of neutron multiplication and hence fission. The Los Alamos Primer describes the underlying neutronics.

In a simplified picture, we note that for any given mass, the neutron multiplication factor (the ratio of neutrons in a generation to a previous generation) can be written as:

$$k = \frac{\text{neutrons produced}}{\text{neutrons absorbed} + \text{neutrons lost due to leakage}}$$

and is a measure of the criticality of the mass ($k > 1$, supercritical; $k = 1$, critical; $k < 1$, subcritical. $k \geq 1$ is needed to sustain a chain reaction). The associated rate equation can be written as:

$$\frac{dn(t)}{dt} = \frac{k-1}{\ell} n(t) + s(t)$$

where $n(t)$ is the number density of neutrons ($\#/cm^3$), ℓ is known as the neutron lifetime ($\sim 10^{-6}$ s), and s ($\#/cm^3$ s) is a source of neutrons. The factor k is approximately expressed as:

$$k = \frac{vN\sigma_f}{N\sigma_a + B_g^2 / (3N\sigma_{tr})}$$

where v is the average number of neutrons produced in a fission, σ (cm^2) is known as the cross-section for interaction with neutrons, and the subscripts f , a , t and tr indicate fission, absorption, total and transport cross sections. N indicates the number density of the nuclei ($\#/cm^3$) in the mass, and is obtained as:

$$N = \frac{0.6023 \times 10^{24} \rho}{M}$$

where ρ is the density of the mass (gm/cm^3), and M is the molecular weight ($gm/gmol$). B (cm^{-2}) is known as the geometric buckling, and is a function of the geometry. For a spherical mass of Radius R (cm), this is expressed as:

$$B_s = \frac{\pi}{R + 0.7104 / (N\sigma_{tr})}$$

Thus the factor k can be written as:

$$k(R) = \eta \left(1 + \left(\frac{\pi}{R + \frac{0.7104}{N(R)\sigma_{tr}}} \right)^2 \frac{1}{3N^2(R)\sigma_{tr}\sigma_a} \right)^{-1}$$

Where

$$\eta = \frac{v\sigma_f}{\sigma_a}$$

and is known as the “eta” factor. This would be the value of k if the mass were infinite and thus there was no loss of neutrons due to leakage. Note that for a fixed mass, N is a function of R through its dependence on density, and

$$N(R) = \frac{0.6023 \times 10^{24}}{M} \rho_0 \left(\frac{R_0}{R} \right)^3$$

ρ_0, R_0 are respectively the initial density and radius of the sphere. N will increase with a decrease in R , as $1/R^3$. Thus given a mass, k depends on R in an inverse fashion.

The rate of energy (the Power, P) release in fissions is expressed as:

$$P = G_f (N\sigma_f) (vn) \left(\frac{4\pi}{3} R^3 \right)$$

where G is the energy release (~ 190 MeV) per fission, and v is the speed of neutrons (cm/s). The product vn is referred to as the neutron flux, and corresponds to neutron path length per unit time. Parameters appropriate to fast (~ 2 MeV) neutrons and Pu-239 have the approximate values:

$$\eta = 3.0$$

$$\sigma_a = 1.87 \times 10^{-24} \text{ cm}^2, \quad \sigma_{tr} = 6.0 \times 10^{-24} \text{ cm}^2$$

$$\ell = 10^{-6} \text{ s}$$

Together with

$$\rho_0 \approx 15.5 \text{ gm / cm}^3$$

as the normal density of the Plutonium, one finds that for $k=1$,

$$R \approx 7.0 \text{ cm}$$

This corresponds to a mass of about 22 kg. Refined theory and calculations, with results confirmed by experiments (the Jezebel assembly), show that :

$$R \approx 6.285 \text{ cm}$$

which corresponds to a mass of about 16 kg. This value is substantially reduced if the mass were to be surrounded by suitable reflecting materials such as U-238 and beryllium.

The basic principle then is to:

1. Start with a subcritical mass, or masses (which do not sustain a chain reaction because of a larger proportionate leakage of neutrons from the mass as compared to fission) of the fissile material. This mass is usually spherical or cylindrical in shape, and is encased in Uranium-238, beryllium, or some other materials that reflect neutrons or aid in compression. The reflection reduces the required U-235 or Pu-239 mass by about 50%.

2. Rapidly compress this mass using chemical explosives or a gun type system in which one mass is fired into another. The compression leads to an increase in the density of the fissile material decreasing the neutron mean free path (the mean distance a neutron travels before interaction), and thus fissions become comparatively more favored over neutron leakage from the material. During the compression a stage is reached where a chain reaction can be sustained, and as the compression progresses the number of neutrons and fissions, and hence energy release, can double or more with each incremental increase in time (of the order of 10^{-6} s, a microsecond, the "neutron lifetime"). The energy release doubles with progressively shorter increments of time, since as the compression progresses the mean free path becomes smaller and smaller, and thus the mean free time for fission becomes shorter). Since the released energy will lead to expansion (thermal and pressure), the weapon will start losing its ability to sustain a chain reaction as the expansion progresses and certainly by the time it reaches its original size again. Thus during the compression or assembly phase (the chemical detonation), neutrons are injected at a proper time with an external neutron source, so that the desired number of fissions, and hence energy release, is achieved during the compression and expansion phases combined. Much of the energy release occurs during the last few time increments of the 50 or so fission generations (or the time increments), and thus the criticality should be maintained for as long as possible. The assembly must occur in a fashion that avoids premature detonation (that is release of energy sufficient to cause disassembly, but not sufficient otherwise) by stray neutrons (e.g., those associated with natural, spontaneous production in Pu-240, which is present in small amounts with Pu-239 in the processed material). This requires use of guns that fire at very high speeds (1000 m/s) or rapid (~ a microsecond) and symmetric implosions through shock waves generated by use of chemical explosives. Generally, guns are sufficient for U-235 weapons, but implosion is needed for Pu-239 weapons.

The early fission weapons used polonium (an alpha emitter) and beryllium (which emits a neutron on alpha absorption) to generate neutrons. These materials were initially placed at the center of the sphere, presumably separated by a foil

which absorbs alpha particles and prevents exposure of beryllium to these. The foil is ruptured at an appropriate time in the implosion, leading to neutrons that initiate the explosion. Neutrons can however also be generated through interactions of hydrogen isotopes or other isotopes in small electricity-driven devices (accelerators) that are used these days, for example, in oil exploration.

Fission weapons are characterized by small size; the explosive part is only a few centimeters in diameter. Power density is extremely high, and explosion time is a few microseconds. Commercial nuclear reactors on the other hand are large with cores that are approximately 12 ft in diameter. Their power density is low. Also, energy is produced over a long period of time. Design safeguards protect against power excursions.

SUMMARY

Nuclear weapons inflict vast damage, and must not be allowed in the hands of terrorists or irresponsible parties. Seven nations have announced nuclear detonations and many other nations have the capabilities to produce/announce nuclear detonations on short notice. Some are surely working towards acquiring the capability. The fundamentals of crude nuclear weapons production are reasonably well understood and publicized. The available public knowledge base has increased since nuclear weapons were first produced and used in 1945. Still, nuclear weapon design and assembly is not a task for amateurs as many complicated practical and technical details are involved. The task is less difficult however, for a large, well-organized, and well-financed terrorist organization.

BIBLIOGRAPHY

1. S Glasstone. *The Effects of Nuclear Weapons*. (U. S. Govt. sponsored, first published 1950; 1964).
 2. R Serber. *The Los Alamos Primer*. (U.S. Govt., first published as LA-1, April 1943; declassified 1965; annotated book, 1992).
 3. AC Brown, CB MacDonald. *The Secret History of the Atomic Bomb*. (1977, it includes the Smyth Report which is an official history of the U.S. efforts, 1940-45, completed before the trinity test).
 4. *Project Y: The Los Alamos Story* (Tomash Publishers, 1983, includes U.S. Govt. sponsored *Toward Trinity* by D. Hawkins and *Beyond Trinity* by E.C. Truslow and R.C. Smith).
 5. *Reactor Physics Constants*. ANL-5800. (U.S. Govt., 1963).
 6. R Rhodes. *The Making of the Atomic Bomb*. Touchstone Books, 1992.
-

7. H Morland. *The Secret that Exploded*. Random House, 1986.
8. A McKay. *The Making of the Atomic Age*. Oxford Univ. Press, 1984.
9. GI Bell, S Glasstone. *Nuclear Reactor Theory*. Krieger Publishing Company, 1974.
10. RL Garwin, G Charpak. *Megawatts and Megatons*. Knopf, 2001.
11. W Meyer, SK Loyalka, W Nelson, RW Williams. The homemade nuclear bomb syndrome. *Nuclear Safety* 18: 427, 1977.

15

Nuclear Terrorism: Threats and Countermeasures

Sudarshan K. Loyalka and Mark A. Prelas

University of Missouri, Columbia, Missouri

INTRODUCTION

There is little question now that some terrorists groups are keenly working towards acquiring nuclear weapons, and are also considering attacking/sabotaging nuclear installations. We discuss here the plausibility of these threats and how governments and industry might effectively respond to prevent such terrorism.

THREATS

Motivations for nuclear terrorism exist, both in large terrorist groups and some states. There is likely to be a greater move towards nuclear threats as terrorists exhaust other means and tactics, and as they become more experienced, sophisticated, and knowledgeable. Nuclear threats are plausible as together with motivations, materials and expertise for making crude weapons may be acquired, means for delivery may be available, attacks on nuclear installations or their sabotage may be feasible, and nuclear weapons may be stolen or purchased. Again, in these discussions we will focus on fission weapons.

Materials: The principal issue in assembling fission weapons is with the availability of a few kilograms of “weapons grade” U-235 and Pu-239 metals or their oxides.

Uranium occurs naturally, and it is mined in many places in the world. This natural uranium is composed of 99.3% U-238 and only 0.7% U-235. U-238 can

undergo fission with energetic neutrons, but it also absorbs neutrons significantly, leading to substantially negative impact on the chain reaction and overall fission process, and the requisite mass (one needs larger mass to reduce leakage comparatively). For weapons purposes uranium must be "enriched" in U-235 content to 20% and above, and preferentially 90% and above. This is generally accomplished by conversion of natural uranium to a gaseous hexa-fluoride form, followed by use of an electromagnetic, diffusion, centrifugation, nozzle flow, or laser process.

Acquisition of natural uranium by terrorists should be straightforward. The enrichment technologies are however generally both sophisticated and expensive, given the small mass difference between U-235 and U-238. Electromagnetic and laser separation techniques, however, do not require large investments and expense if the purpose is to produce limited quantities of weapons grade uranium.

Pu-239 is not available naturally (although some of it certainly was produced at one time in the natural reactor in Gabon, millions of years ago). Rather it is produced, together with its higher isotopes some of which are a weapon maker's nightmare, through absorption of neutrons in U-238, and subsequent radioactive decays (transmutations), and processing of irradiated uranium. The neutron irradiation can be carried out in neutron accelerators and nuclear reactors. In the Manhattan project, such reactors were constructed using natural uranium and graphite or heavy water. Many such reactors are now in commercial use, and these, and other reactors that use slightly enriched uranium (2-4% U-235), do produce Pu-239. But this plutonium is also contaminated with Pu-240 which produces neutrons by itself (spontaneous fissions), and is not good for weapons purposes. The weapons grade plutonium should have 5% or less of Pu-240, and should be mostly Pu-239 to prevent premature explosions of weapons (in a plutonium-based weapon, implosion is necessary to counter premature disassembly due to neutrons produced by Pu-240). This purity could be realized by short term irradiation of U-238 in research (or commercial) reactors and appropriate processing of the irradiated material. One might also use other neutron generators, e.g., accelerators, to irradiate natural uranium, and obtain Pu-239. But this latter route is not a very effective way to produce kg quantities.

Diversion and theft of U-235 and Pu-239 from national nuclear weapons programs as well as the fuel cycle (manufacture, shipment, use, reprocessing) associated with research and commercial nuclear reactor plants is the main vulnerability. Fresh commercial reactor nuclear fuel is enriched only to 2-4% in U-235, and is not an issue. The used fuel contains Pu-239, but it is radioactive and is also heavily contaminated with Pu-240. Terrorists could disperse radioactivity in such fuel by using chemical explosives, but separation of Pu-239 from this fuel for an effective fission weapon will be very difficult. There are some research reactors that use 93% U-235 or so enriched uranium fuel (known as Highly Enriched Uranium-HEU), and there are also commercial reactor plants that use Pu-239 based fuel. Fresh fuel here could provide sufficient quantities of weapons grade U-235 or Pu-239.

Of course, an actual weapon could also be stolen, diverted, or purchased. While all nuclear nations have safeguards, the sheer number of weapons stockpiled by the major nuclear nations, and political instabilities of some other nations that have smaller stocks, do not provide strong assurances against such eventualities.

Up until 1991, the security of nuclear stockpiles and weapons know-how was not a significant concern. However, it quickly became a concern when the Soviet Union collapsed. The Soviet Union had accumulated between 140 to 160 metric tons of plutonium and a considerably larger inventory of HEU [1]. Under the circumstances of a collapsing economy, the once elite weapons designers of the Soviet Union were facing poverty and hardship. The security of nuclear materials and the potential for the migration of know-how to rogue states was of great concern to many in the west [2].

Expertise: Actual design of a workable explosive requires sophisticated analysis and synthesis, is a work for serious professionals, and is classified. The metallurgy and machining of various materials and components, work with explosives, electronics, neutron sources, and radiation also require equipment and experienced scientists and engineers. Powerful computers are now ubiquitous. Sophisticated computer programs that deal with neutronics, fluid dynamics, heat transfer, and structural issues are also widely available.

It appears that three to five scientists and engineers, with diverse expertise in nuclear physics and engineering, metallurgy, explosives and electronics are the minimum that would be needed. This team would need access to computers, good laboratories, machine shops, and testing facilities.

The expertise can be developed or acquired while a group is pursuing acquisition of the material. The dissolution of some national nuclear weapons programs has created a large pool of unemployed or disaffected weapons specialists, and some of them could be recruited.

Targets and Means of Delivery: Targets of nuclear terrorism would be large cities and infra-structure, private and public. Nuclear weapons are rather compact, and could be delivered by air, water or land. Of these, the last two may be more attractive to terrorists as barges/ships can be sailed into harbors, and trucks/trains can be driven into cities or near other defense/government facilities and other industry with smaller likelihood of detection. One could also transport parts of a weapon at different times to thwart detection, and then assemble the weapon at the site.

Nuclear installations (manufacturing and storage facilities, nuclear power plants, research reactors) and shipments (raw material, fresh fuel, used fuel) are all plausible targets for acquisition of nuclear material, or attacks that could lead to release of radioactivity from these installations or activities. Nuclear power plants are often located in remote areas and research reactors contain relatively small amount of radioactive material. Neither are likely to undergo a nuclear explosion excepting special circumstances, but chemical explosions/fires or plane crashes at

these sites can cause great difficulties, and eventual release of radioactivity and harm.

COUNTERMEASURES

Countermeasures against the nuclear threats must be general as well as very specific. Both short and long term steps are needed, and these must be vigorously implemented. The greatest concern is with respect to acquisition of the weapons grade nuclear material, and spread of technology that makes its production possible given natural uranium. There are concerns with the spread of expertise of weapon making, but given the large number of trained scientific and technical personnel and scientific/industrial facilities and laboratories these days, there is only so much that can be done in this area. In the short run the countermeasures must:

Protect Nuclear Weapons: All nuclear nations safeguard their nuclear weapons, but there is unevenness that must be addressed. In order to safeguard nuclear weapons, a number of Arms Control treaties have been developed. We will describe a few of these and their interlinks and implications to nuclear security.

After the Cuban missile crisis, both the US and the USSR realized the folly of a nuclear arms race. Even though the earliest efforts to limit nuclear arms met with little success, it did lay the groundwork for the future. The issue early on was how to achieve comprehensive disarmament. At the Geneva-based Eighteen-Nation Disarmament Committee in January 1964, the US proposed that the number and characteristics of the strategic nuclear offensive and defensive delivery systems be decoupled from the comprehensive disarmament proposals. By 1966, China developed nuclear weapons, and both the USSR and the US were engaged in the development of anti-ballistic missile systems. In 1967 it became clear that the nuclear arms race was unmanageable and President Johnson and Premier Kosygin indicated a willingness to reengage in arms control discussions. By July 1, 1968 the Non-Proliferation Treaty was signed and the US and USSR agreed to initiate discussions on the limitation and reduction of both strategic nuclear weapons delivery systems and defense against ballistic missiles. The Strategic Arms Limitation Talks (SALT I) occurred from November 1969 to May 1972. SALT I ended when both the US and the USSR signed the Anti-Ballistic Missile treaty on May 26, 1972 and developed the Interim Agreement on Strategic and Offensive Arms (agreed to begin talks for a more comprehensive nuclear arms treaty) which led to the SALT II talks and the signing of the SALT II treaty on June 18, 1979. The SALT II treaty would have limited nuclear delivery vehicles (missiles, bombers and air to surface anti-ballistic missiles) to 2400 units. The treaty was not brought to the senate for ratification, but both countries agreed to abide by the provisions. President Reagan stated that the USSR was not in compliance with SALT II in 1986 and asked USSR to join with the US in mutual restraint. One of the major issues with SALT II was verification, a theme that persists to this day.

Arms control made progress in the 1980s through the Intermediate-Range Nuclear Forces (INF) Treaty that was signed on December 8, 1987. The START I treaty was undertaken with regard to strategic offensive arms in Article VI of the Treaty on the Non-Proliferation of Nuclear Weapons of July 1, 1968; Article XI of the Treaty on the Limitation of Anti-Ballistic Missile Systems of May 26, 1972; and the Washington Summit Joint Statement of June 1, 1990. The START I treaty was signed in Moscow on July 31, 1991. With START I, the U.S. and Russia agreed to reduce strategic nuclear warheads to 6000 [3]. In December 1991, the USSR disbanded and became the Commonwealth of Independent States (CIS). On May 7, 1992, Each of the Commonwealth States that housed nuclear weapons agreed along with US to abide by START I in the Lisbon Protocol. START II was designed to reduce the level of strategic nuclear warheads to 3500 and was signed on January 3, 1993. However, START II has not been ratified by the US but has been ratified by Russia. Another milestone treaty was The Comprehensive Nuclear Test-Ban Treaty (CTBT), which halts nuclear testing. CTBT was signed on September 24, 1996 but was rejected by the U.S. senate in 1999. The reason being that nuclear deterrence is still an important component of the U.S. strategic arms package. Nuclear weapons are complex systems that require extensive testing. Without testing, the current nuclear inventory would age and there would be no mechanism for developing replacements.

When the USSR dissolved and the CIS was established, the future of the treaties that served as the foundation of arms control came into question. The first issue was how to deal with START I since some of the states other than Russia in the CIS housed nuclear weapons. The Lisbon Protocol was initiated to assure that these states still agreed to START I. Additionally, these states agreed to transfer control of the nuclear weapons on their territory to Russia. The next issue was to deal with the security of nuclear materials and with the large number of Former Soviet Union scientists engaged in the nuclear weapons enterprise. One of the first steps was to create the International Science and Technology Center (ISTC) by President Bush in 1992. The goal of the ISTC was to support Former Soviet Union (FSU) scientists engaged in the production of nuclear, chemical and biological weapons in projects for peaceful uses and economic development. The US, Japan and the EC committed 75 million dollars to initiate the program. In addition, the (George) Soros Foundation provided a large amount of money to support FSU scientists. Soros eventually started the International Science Foundation to support FSU scientists and this project eventually evolved into the Civilian Research Development Fund. To safeguard FSU nuclear stockpiles the Nunn-Lugar bill supported efforts to foster Russian warhead dismantlement, work on surplus fissile material disposition options, lab-to-lab cooperative non-weapons projects with Russian nuclear scientists, and support of the Russian highly-enriched uranium purchase agreement. In addition the US provided funding to the Mayak Production Association for the construction of a plutonium storage facility. The goal of these efforts and others was to help Russia secure its nuclear materials stockpile. To date, the program has been successful in a number of areas. It has provided sup-

port to critical FSU scientists in order to secure the scientific know-how for the production of nuclear weapons plus it has helped Russia with funding to develop better methods of nuclear stockpile stewardship.

Under the leadership of the Bush administration, the U.S.-Russia Strategic Offensive Reductions Treaty was signed on May 24, 2002. This landmark agreement will cut the number of strategic nuclear warheads to between 1,700 and 2,200. This reduction is lower than the reduction goals of the START III talks, but unlike START III, the U.S.-Russia Strategic Offensive Reductions Treaty will allow for the storage of nuclear materials from old warheads.

While the two nations are reducing their stockpiles, some other nations are building theirs although not up to the same levels. These large numbers lead to possibilities that some weapons are not fully accounted for, and that there can be unrecognized theft from storage or during weapon transfers. The best strategy here is to reduce nuclear stockpiles, account for all weapons, and share and adopt good security practices.

Protect Nuclear Materials: All nuclear material from mining to its eventual disposal must be fully accounted for and guarded by public agencies in all nations. The weapons grade material (HEU and Pu-239) must receive the highest level of protection. High level of protection should be provided to fresh nuclear fuel. Irradiated fuel in most instances is self protected, but it would contain Pu-239, and since such fuel can itself be a source of release and a terrorist tool because of radioactivity content, it also deserves similar level of protection. The greatest difficulty in this area has been reported with respect to transitions that have occurred with the dissolution of the former Soviet Union, and extensive material stocks that had existed and that are not fully accounted for.

Control Nuclear Transfers: Transfer of nuclear material to unstable states, or states that are prone to cooperation with terrorists, must be stopped.

Protect Nuclear Expertise: There is a vast difference in the theory and practice of weapons technology, and the greater emphasis here must be on ensuring that terrorists do not get access to the technology or the experienced practitioners in the field. Dual use technology should be clearly identified, and its commerce regulated. All present and former weapons scientists should be provided some stable financial support so that they do not find it necessary to help terrorists because of financial hardships.

Destroy Nuclear Infrastructure: Israel destroyed the Osiriak reactor in Iraq in 1981 to prevent what it viewed as the development of a nuclear weapons infrastructure in Iraq. There have been reports of assassinations of some nuclear weapon experts also. These are obviously strong measures, and have not been used widely.

Upgrade Intelligence Programs: Nuclear weapons materials and technology can be acquired in parallel, and often under the guise of legitimate peaceful work. Intelligence programs should be reviewed, and capabilities developed not only for providing support towards prevention of thefts, etc., but also to anticipate and constraint dual use operations.

In the long run, all the above steps will need to be strengthened. Regulations, intelligence, and interdiction (emergency response) are essential to prevent nuclear material from reaching the hands of terrorists. In the U.S., the Department of Energy, the Nuclear Regulatory Commission, and the Defense Department have the primary responsibilities for regulating the nuclear material and activities. Other nations have similar organizations that deal with this issue. The International Atomic Energy Agency based in Vienna, Austria provides international regulations and oversight, and cooperation among different nations. In a sense, the very extraordinary nature of nuclear threat has fostered national and international regulation from the beginning and it continues to date. There is a need to strengthen the regulations, and also to ensure some minimum uniform compliance with them globally. The international community must engage more strongly in nuclear arms control and nuclear arms reduction. It must jointly ensure reduction of nuclear terrorist threat worldwide by cooperating in regulation, intelligence, and interdiction.

SUMMARY

Nuclear terrorism could comprise attacks against nuclear installations, and dispersal of radioactive materials from storage, shipment, nuclear reactor fuel, etc. through use of conventional explosives and other means, as well as acquisition and use of nuclear weapons. The threat of fission weapon construction/ acquisition and use by terrorists has become more credible with the spread of nuclear technology and international instabilities and dynamics. Given the material, a crude bomb could possibly be built by a small team of scientists and engineers with diverse experience. Protection of weapons and Highly Enriched Uranium and Pu-239 require the highest level of understanding and international cooperation. Regulations, intelligence, and interdiction on a national as well as global level can provide the needed safeguards.

REFERENCES

1. World Plutonium Inventories, 1999. Bulletin of the Atomic Scientists, Vol. 55, No. 5, page 71 (<http://www.thebulletin.org/issues/nukenotes/so99nukenote.html>)
2. M Prelas. Soviet High-Tech Bonanza. Christian Science Monitor, 02/03/1992, (<http://www.csmonitor.com/cgi-bin/getasciiarchive?tape/92/feb/day03/03181.>)
3. Strategic Arms Reduction Treaty (START I). US Department of State, (<http://www.state.gov/www/global/arms/starthtm/start.html>)

BIBLIOGRAPHY

P Leventhal, Y Alexander. Nuclear Terrorism, Defining the Threat. Pergamon, 1986.

P Leventhal, Y Alexander. Preventing Nuclear Terrorism. Lexington Books, 1987.

Safeguards Against Nuclear Proliferation, A SIPRI Monograph. MIT Press, 1975.

Nuclear Proliferation Problems, SIPRI. MIT Press, 1974.

Nuclear Proliferation and Safeguards. Office of Technology assessment, Congress of the United States, Praeger Publishers, New York, 1977.

16

Cyber-terrorism

Harry W. Tyrer

University of Missouri, Columbia, Missouri

THE NATURE OF CYBER-TERRORISM

Terrorism elicits terror – not inconvenience, nuisance, or concern – but, terror. However, terrorism must have a purpose, one uses terror, violence, and intimidation to achieve an end. The system of government may use a system of terror to rule, and they would use fear and subjugation to achieve these aims. Those opposing a government may use terror to coerce public opinion to achieve their aims. A formal definition comes from the United States Department of State:

The term terrorism means pre-meditated, politically motivated violence perpetrated against non-combative targets by sub-national groups or clandestine agents.

Norbert Wiener, the well-known MIT mathematician who developed the Wiener–Hopf equation for signal filtering, coined the term Cybernetics for the title of his book. Cybernetics is Greek for steersman and it is the name Wiener and his colleagues gave to the entire field of control and communication, whether in the machine or animal. Wiener justifies his choice of terms based upon a paper by Maxwell on feedback dated 1868, where Maxwell used the term governor, a Latin corruption of the Greek steersman. To Wiener and colleagues an essential aspect of control is the communication required to change the control, in other words feedback. And cybernetics arose in the context of feedback in control systems. We may presume that cyber is a popular corruption of Cybernetics. (Incidentally, Wiener was born in Columbia, Missouri, where his father was a professor of linguistics at the University.)

On the other hand, cyber-space refers to the vague entity of human communication using computers and their power as a medium. Cyber-space is not merely telephone lines, but the additional intelligence that is available by computational means. While e-mail is certainly considered a component of cyber-space, e-mail alone is not cyber-space. Cyber-space includes the communication of computing resources directed toward some end, usually requiring and transmitting intelligence. Additional components include the world-wide-web and even such new technologies as agent-directed intelligence.

DEFINITION OF CYBER-TERRORISM

Cyber terrorism then is a coinage that involves both cyber-space and terrorism. Additionally, there are some who believe cyber-terrorism must contain a political component as the end for which cyber-terrorism is the means. Pollitt has proposed that cyber-terrorism is the pre-meditated, politically motivated attack against information, computer systems, computer programs, and data, which results in violence against non-combative targets by sub-national groups or clandestine agents.

However, this definition fails to explicitly take into account the severity of terrorism. Indeed, some have proposed that cyber-terrorism is the use of information technology to disrupt critical infrastructure. This definition expands the scope of cyber-terrorism to include those elements, which may be controlled by the information technology resources.

A useful definition comes from Deming, who considers cyber-terrorism to be the convergence of terrorism and cyber-space. By that she means the unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people and furtherance of political or social objectives. Deming believes that to qualify as cyber-terrorism, the attacks should result in violence against persons or property, or at least cause enough harm to generate fear.

For our purposes here, cyber-terrorism involves the use and abuse of information technology to generate violence, damage, and fear. Cyber-terrorism, then, is the use of information technology to effect violence directly on or indirectly on an infrastructure and resources, and to generate fear in people directed toward some political aim.

DISTINCTIONS

Deming also provides an interesting softening of cyber-terrorism in using the term "hack-activism". Hack-activism combines hacker with activism. Here, the severity of the damage ranges from nuisance to just before generating fear. Most writers up to the current time (spring 2001) feel that the world has yet to experience an act of cyber-terrorism. The plain fact is that terrorism of the non-

cyber variety, is much more effective than the nuisance value of turning out the lights.

While some apologists for hackers have tried to paint hackers as the good guys, and crackers as the bad guys, the fact is that such distinctions are useless, and hackers cannot control the collateral damage that they impose, and usually have little ability to curb the damage that they have initiated. The best examples are the shutting down of a large number of military computers, and the "I Love You" e-mail virus, and its variants. Both acts caused a large amount of damage that was beyond the control of the hackers perpetrating such acts, and netted these hackers criminal liability.

The broadness of the definition of cyber-terrorism requires its distinction from hack-activism. That distinction is the threshold of the violence imposed by Deming; it delineates those activities that should correctly be called cyber-terrorism. Unfortunately, the tools used by the hacker and the cyber-terrorist are the same or similar. It is a matter of degree rather than substance.

The Stories

Hacking, in fact, is starting to become more than just a simple nuisance or a prank. It is worthwhile to consider the experience of this writer in the recipient of hacking activities.

A security log was obtained from a workstation in which four different entities attempted to log into that workstation.

```
From root@xx.yy.missouri.edu Wed Aug 22 13:51:33 2001
Date: Sat, 16 Dec 2000 07:00:03 -0600 (CST)
From: Super-User <root@xx.yy.missouri.edu>
To: a@missouri.edu,
    b@missouri.edu,
    c@missouri.edu
Subject: zz: Daily Security Report
```

```
Dec 10 20:43:36 4C:ww ftpd[29955]: refused connect from cm47580-
a.ftwrth1.tx.home.com
Dec 11 10:37:36 4C:ww ftpd[2008]: refused connect from acn.pl
Dec 11 22:08:34 4C:ww telnetd[3698]: refused connect from adsl-216-
61-33-41.dsl.austtx.swbell.net
Dec 11 22:08:40 4C:ww telnetd[3704]: refused connect from adsl-216-
61-33-41.dsl.austtx.swbell.net
Dec 11 22:08:45 4C:ww telnetd[3710]: refused connect from adsl-216-
61-33-41.dsl.austtx.swbell.net
Dec 11 22:08:50 4C:ww telnetd[3716]: refused connect from adsl-216-
61-33-41.dsl.austtx.swbell.net
Dec 11 22:09:13 4C:ww telnetd[3723]: refused connect from adsl-216-
61-33-41.dsl.austtx.swbell.net
Dec 12 02:21:57 4C:ww telnetd[4293]: refused connect from modem-68-
14-60-62.vip.uk.com
Dec 13 16:58:03 4C:ww ftpd[9902]: refused connect from san-
ity.ece.wisc.edu
```

```
Dec 13 17:09:17 4C:ww ftpd[9941]: refused connect from
h002078c7355d.ne.mediaone.net
Dec 14 17:27:39 4C:ww ftpd[13442]: refused connect from lane0002-
44-3.coburg.eug.clipper.net
Dec 14 18:19:52 4C:ww ftpd[13576]: refused connect from lane0002-
44-3.coburg.eug.clipper.net
Dec 15 08:22:43 4C:ww ftpd[15480]: refused connect from
www.ls.utp.ac.pa
Dec 15 12:42:03 4C:ww ftpd[16234]: refused connect from evrtwal-
ar4-155-070.biz.dsl.gtei.net
Dec 15 15:13:44 4C:ww ftpd[16589]: refused connect from
h170n2fls20o93.telia.com
Dec 15 19:57:56 4C:ww ftpd[17241]: refused connect from
mail.genericad.com
Dec 15 20:48:29 4C:ww ftpd[17362]: refused connect from
mail.genericad.com
Dec 15 21:15:53 4C:ww ftpd[17432]: refused connect from ds1254-084-
111-nycl.dsl-isp.net
```

None of these activities were legitimate, and neither station name, nor the IP address has any meaning to the hacked workstation. Furthermore, an examination of the logs over several weeks shows an attempt to surreptitiously gain access to this workstation by a large number of different people. The recipient of this activity feels violated, not unlike the feeling when one's home is burgled. This is, of course, not an isolated case. There have been recent reports describing that PCs connected to telephone lines have been accessed, and DSL with its always-open line is well known to be insecure. This is compounded by the fact that Windows systems for the home market have no access control.

When one receives an e-mail from an individual whose subject line is completely out of character, there may be problems lurking. The email exchange below shows that the variant of the "I Love You" bug caused severe damage to the recipient.

```
From a@bbb.edu Wed Aug 22 13:47:38 2001
Date: Thu, 28 Sep 2000 13:55:40 -0500
From: ab < a@bbb.edu >
To: cd
Subject: Re: Did you send me a joke?
```

No, I did not. It accessed my system. I lost 5,000+ files.
So sorry.

```
----- Original Message -----
From: cd
To: ab < a@bbb.edu >
Sent: Thursday, September 28, 2000 12:57 PM
Subject: Did you send me a joke?
```

```
> a
> I was much surprised to receive two emails from you with subject
heading
```

> joke. Our email protection programs found one and deleted it,
that may
> not mean anything. If you sent it, then I'll be glad to read it.
I am
> concerned though that your machine is being used as a pawn in
someone
> else's joke.
>
> Cordially,

These two incidents point out the collateral damage done by hackers. This damage serves to tie up communication resources, destroy work that has taken time to perform, require effort to correct the situation and lose irreplaceable material. Hackers typically justify this in terms of teaching the need for security, which is of course a fundamentally corrupt notion. The fact is that security is only as good as the means of unauthorized access it prevents: a sturdy wooden door protecting a home is no match for battering ram which is no match for a metal door and so on.

More to the point are attacks in furtherance of political and social objectives that include the following:

1. A Massachusetts ISP was disabled, and part of their record keeping damaged by a hacker associated with a white supremacist movement.
2. Spanish protestors bombarded the Institute for Global Communication with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to associated users.
3. Tamil guerillas swamped embassies in Sri Lanka over a two-week period with around 1,000 e-mails a day.
4. During the Kosovo conflict of 1999, NATO computers were blasted with e-mail bombs. Denial of service attacks with a political message screen web-sites conducted with sit-ins in support of the Mexican uprising in Chiapas. In this technique, thousands of protestors point their browsers to a target site at a given time. The software floods the target with rapid and repeated download requests. Similar web incidents occurred against WTO in Seattle.
5. In the Arab-Israeli conflict, there are numerous incidences of hacking, but none have been classified as cyber-terrorism. The primary damage is breaking into and modifying the web site hacking mail services effecting a distributed denial of service. Furthermore, denials of service in various important Israeli government sites have been affected.

Interestingly, under British Law cyber-terrorists, which includes hackers, are to be treated the same as any run-of-the-mill terrorist. Measures have been written into the definition of terrorists as anyone who tries to seriously disrupt an electronic system with the intention of threatening or influencing the government or public, and to advance a political, religious, or ideological cause, are considered cyber-terrorists.

WHAT IS REAL?

The CIA has set up a group to simulate the shutting down of government computers using tools available to hackers on the world-wide-web. They were able to shut down a large number of computers, and demonstrated that there was a high level of vulnerability. It should be noted that the potential for vulnerability and the acting upon this vulnerability are two different things.

There is a substantial amount of crime perpetrated that is not cyber-terrorism. Nevertheless, the tools that are used are the same. A recent story involved a 16-year old manipulating the stock market, but he was caught by the FCC, and required to pay nearly \$300,000 in fines. The crime? The student was hyping stock, and then selling to the unsuspecting buyers.

There is more hype than fact in most articles dealing with cyber-terrorism. Typically, the story identifies a weakness, and builds upon that weakness. Recently, the National Security Advisor to President Bush, Condoleezza Rice, indicated that the government must work more closely with private companies to prevent cyber-terrorist attacks that threaten to disrupt the nation's economy. She was quoted as having said: "Today, the cyber-economy is the economy; corrupt those networks, and you corrupt this nation." The fact is, of course, that there is a substantial simplification in these statements that, in fact, does not follow. It seems clear that substantial effort must be generated to disrupt the economy, and that is a substantial task.

Furthermore, communications systems are complex, so it is hard for a perpetrator to control an attack, and the drama and emotional appeal is quite low, unless one causes injury. Furthermore, writers seem to believe that terrorists are disinclined to try new methods, unless there is a good reason to do so. Finally, the level of automation is insufficiently high that it is possible to impose wide-scale damage without human intervention. Knocking down a power grid, causing a nuclear plant meltdown, or sufficiently disrupting airplane flight to cause damage, is sufficiently in the future that appropriate preparations can be made.

The Naval Post-Graduate School, in Monterey, California, assessed the prospects of terrorists pursuing cyber-terrorism. They concluded that the barrier for entry for anything beyond annoying attacks is quite high. They defined three levels of cyber-terrorism capability.

1. Simple, unstructured: Hacking with tools.
2. Advanced, structured: Sophisticated attacks against multiple systems, using elementary target analysis, command and control, and learning capability.
3. Complex, coordinated. The capability for coordinated attacks capable of causing mass disruption against integrated, heterogeneous defenses. They estimate that, starting from the beginning, to reach the complex coordinated level, would require on the order of 8 to 14 years.

It seems clear from this analysis that a large number of people have an interest in hacking and disrupting communications, even to see if they can “just do it”, which may be their only motivation. There is a baseline of hacking activity, which is more nuisance than anything else; nevertheless some of this actually becomes fraud. The cyber-terrorism that the world has experienced so far is simple and more hack-activism than cyber terrorism. Nonetheless, continuing improvements in technology and in the hacker’s trade should motivate organizations and governments to protect themselves against future terrorism. If we assume that the popular Internet started with the creation of Netscape in 1994, then the complex coordinated level of cyber attack can be expected to begin from 2002 to 2008. It is not difficult to image that in 20 years (2021) the continued emphasis and training in computing will provide a cadre of dedicated computer literate cyber-terrorists.

UBIQUITOUS COMPUTING AND ITS VULNERABILITY

As we write this at the beginning of the 21st Century, computing has evolved from a toy in certain niches, and even an important tool, to a necessary part of the communications infrastructure. This communication infrastructure transcends a country’s borders. For a typical message, we can find out who is the sender, and who is the receiver, but we typically do not know the path that the message might have taken. Someone in Columbia, MO can receive an e-mail message from either Germany or the Philippines, with as much ease as they can receive that message from Kansas City, or St. Louis. And because a shortest-path algorithm routes messages, a message from Columbia to Kansas City is unlikely to go east to west: St. Louis, Buffalo, New York, London, Frankfurt, New Delhi, Tokyo, San Francisco, and then finally to Kansas City. Electronically, the United States East Coast is 18 milliseconds away from the West Coast.

Furthermore, as of this writing, there are over 200 million installed personal computers in the world. In the United States, one-half of all families have at least one personal computer. However, it is usually forgotten that this is 2% of the installed base of all computers. The other 98% are embedded computers, which provide the controlling mechanism to a wide variety of equipment. Let us consider the totality of computer systems in terms of their user classification.

EMBEDDED SYSTEMS

A computer is “embedded” into a stand-alone device to control the operation of the device. The software is usually provided by firmware and the operation of the system is in a never-ending loop. The system starts, set to the first instruction, executes all instructions in order, returns to the original first instruction, and executes the instructions in order again. It continues until the device is no longer operating. In more complicated devices, such as an airplane, there may be sub-loops

within the loops. The sub-loops become effective when the operator actuates a particular sequence of operations. Embedded systems commonly implement real-time systems. Real-time is defined as the execution of a particular process within a given time constraint. Many of these devices are taking advantage of the Internet and other networking infrastructure to receive remote signals for operation. There are embedded computers in automobiles to achieve an optimal operating point by controlling the rate of gasoline flow and the production of the spark. Computers in airplanes as controlling elements have clearly demonstrated the substantial improvement in performance of fighter jets. In consumer electronics, computer-control VCRs and compact disc systems. Furthermore, services such as broadband access and web PC, are provide communication and control.

Personal Computers

The wide range of personal computers exists in the home and businesses, small and large. The desktop and laptop units form an infrastructure connected via the Internet, which allows many of these devices to communicate with each other. The Microsoft Windows Operating System on the majority of these machines is very weak in providing security resources.

Personal Device Assistants (PDA)

These hand-held devices are used extensively for note taking and time management systems. Some have wireless networking capability that allows access through the Internet to the larger systems for either upload or download of relevant files. One class of these devices is cell phones with web access, which we will not discuss further.

Corporate and Enterprise Intranets

Business, universities, and other enterprises may connect some or all of their computers together into a set of local area networks. The topology of choice is usually the client server system with any single workstation able to perform the function of both client and server. Furthermore, the connectivity in the same local area network allows all interconnected devices to communicate. Within the Intranet, all networks are allowed to communicate. And, all connected workstations may have access to the single server connected to the Internet.

Super-Computing Clusters

Reminiscent of the typical technology of the 70s where a single large computer served the needs of all the users, very powerful machines exist within organizations to support the high performance computing required for advanced applications. The best-known examples are the San Diego Super Computer Center, and the National Center for Super Computer Applications at the University of Illinois. These facilities have machines capable of operating at teraflops per second (1012 floating point operations per second). These types of machines are available typi-

cally at a single location within a business or military installation. Thus, it is imperative that such machines facilitate remote communication since putative users will typically exchange data with their local machines and the super computer electronically.

So, there are a lot of computers, and they are connected together. Let us focus the rest of this lecture on issues devoted to the individual processor, and in the next lecture we will deal with issues devoted to the network.

SOFTWARE THREATS

The recent rash of highly publicized software threats belies the multi-decade existence of such malicious programs. What has changed is the ubiquity of computing, making software threats a common problem. Further, the pervasive intercommunication between computers allows loading computers with these malicious programs to effect whatever damage is desired.

There are six recognized classifications of this threatening software. They are as follows:

Trapdoor: A bypass of the security framework of a program. Typically, developers place trapdoors in programs under development to more rapidly get into the program's operation. They intend to remove these aids after the development is complete. Occasionally, the developer may leave such security holes available for future use, and only the developer knows about their existence.

Logic bomb: This is an internal piece of code, which activates upon a condition, such as date and time, or an event. An interesting logic bomb used the absence of two sequential paychecks to the developer, in which case the program would self-destruct.

Trojan Horse: As the name implies, the malicious program masquerades as a beneficial program. It may then spawn a logic bomb or another form of maliciousness. The Trojan horse may be embedded into a program, or it may be communicated similar to a worm.

Worm: An agent going from computer to computer to implement the malicious program is a worm. It may then spawn a further malicious program.

Bacteria: These are programs that primarily replicate themselves, and contain no damaging code. The damage from the bacteria comes from the exponential growth of the replication, which will eventually overload resources including memory and disk storage.

Viruses: Certainly the most common of the malicious programs, and the generic name given incorrectly to most forms of software threats. A fundamental property of the virus is that it must attach itself to a program so that it can spawn further. A virus goes through a dormant phase, where it is idle. It then enters a propagation phase, where an identical copy of the virus is placed into other programs or certain system areas, such as the disk boot block. In the triggering phase, the virus is activated to perform its intended function, and finally, during the exe-

cution phase, the function is performed. A virus attaches itself to another program, and executes when the host program is run. The viruses may attach to data, or programs, but must have an execution portion. This damage ranges from a benign message to the screen, to the destruction of files and/or the system.

Table 16.1 Software threats and their properties.

	Penetration	Hosting by	Infection	Infection means
Trap Doors	Inside	Program	None	None
Logic Bombs	Inside	Program	None	None
Trojan Horse	Inside /Communication	Program/none	Yes	None
Worms	Communication	None	Yes	Communication
Bacteria	Communication	None	Yes	Comm / Disk
Virus	Communication	Program/data	Yes	Comm / Disk

Table 16.1 shows each of the software threats and some of their properties. The perpetrator of a software threat may be an insider, that is, a developer or someone who has access to the source code. In contrast malicious programs or software threats which communicate can attach onto other programs. The hosting requirements of these malicious programs may be data, programs, or they may be independent. Typically, a malicious program requires some means of execution; and the easiest way to ensure execution is to attach it onto a program. On the other hand macro viruses common in Microsoft Word systems attach to data (i.e., a word file or .doc file). But the virus is a macro, which executes with the document, usually when the document opens. Finally, there are a number of independent entities, and reside as self-contained programs on the system without attachment to either program or data.

Most software threats have an infection capability. That is, they exist on a system or some medium and then proceed to propagate themselves through the same medium, or through the network connectivity. The exceptions are trap door and logic bombs, which inherently require a host program for implementation, and have no inherent replication capability. Trojan horses and worms typically infect by network communication, whereas viruses and bacterias can pass their infection by disks, or attachment to programs.

Pathologies in computer systems usually become apparent by reduced performance. This translates to the system slowing down. Slow-down can be effected by overloading memory, and storage such as a disk. Additionally the processor may be given too many programs to execute, having the effect of slowing the system. But it is the surreptitious malicious program that may do the most damage.

After all the computer needs to execute to invoke the effect of a program. These can be used to alter the operating system's data structures and changing its effect by producing unpredictable results. It should be clear that there is very little that can be done to physically damage a computer work station. However one can do substantial damage to the operating system and software in the system.

Worse, the sophisticated cyber-terrorist can surreptitiously enter a computer can use the computer as a weapon to wreak havoc in a major way. This requires internetworking such as that available in the Internet.

THE VULNERABLE NETWORK

How does the network facilitate the opportunity for cyber-terrorism? That is, how does a cyber-terrorist inflict damage on the networking system? To do this, we must evaluate networks and their performance from a fairly high level.

A network protocol is the agreement – or standard – defining how two or more computers will communicate. It is assumed that the function “to send” begins with data in a user application. The data are formatted into an integer number of units, and converted to a signal that traverses by either cable or wireless means. The receive function requires the inverse of the sender's operation be performed. That is, signal converted to data, data appropriately formatted to form the message, and finally, acceptance by the user application. The user application can be the user communicating through the operating system.

The network protocol is enshrined in a standard, and there is a bewildering array of standards depending upon the type of data transfer, whether voice, video or data communications. Each has its own set of requirements.

Data communication requires only that data be sent and restored at the destination. Typically, a single interaction is called a message, and the message is broken up into variable length packets, which are the units of data transmitted throughout the network.

In audio communication, the fixed-length packets must be transmitted in order, received in order, and made available to the user at a fixed rate; otherwise, audio distortions will occur. While a single packet loss may be tolerable, neither out of order packets nor variable delays can be tolerated.

Video suffers from the same constraints as audio, namely, fixed-length packets must be transmitted in order and they must be played back to the user within a certain delay time. Video, because it has more information than audio, requires substantially greater bandwidth and tighter specifications. While the loss of one or two packets spaced far apart is tolerable, variations in packet order and jitter in arrival time are not tolerable.

THE COMPONENTS OF COMPUTER NETWORKS

As in all computing applications, software and hardware intimately interact to produce an effect. We will show the relationship between the seven-layer ISO/OSI reference model and a much simpler three-layer architecture. We describe the memory and hardware layout of a typical networked computer so the relationship between memory and network adapter becomes clear. Then we show the contents of the packet, and the code that allows two connected computers to communicate.

It is useful to compare the International Standards Organization/Open Systems Interconnect (ISO/OSI) seven-layer standard to a much more simplified three-layer standard. We will use this three-layer standard throughout our discussion here.

Three Layer Model	ISO/OSI 7 Layer Model	Internet
Local	Application Presentation Session	
Network	Transport Network	TCP IP
Communication	Data Link Physical	

Figure 16.1 Three-layer ISO/OSI standard.

Figure 16.1 shows the seven-layer ISO/OSI standard, and the corresponding three-layer standard. It also shows the layered architecture reference model for TCP/IP. The three-layer model is defined as follows.

In the local layer, the system accesses users tasks and the operating system. It is here that the initial standardization of, say, a video strain takes place. This is passed to the network layer.

The network layer provides the end-to-end communication, routing, and congestion control in an end-to-end sense. Typically, the local layer organizes the data to be transmitted in such a way that the network layer may gain access to them to provide for the resources that it needs.

The communication layer takes the packet from the network layer and converts it into a signal so that the physical electrical data connection can be made.

In terms of the operation of the computer, the following figure shows the relationship between the operation of the computer and the three-layer model.

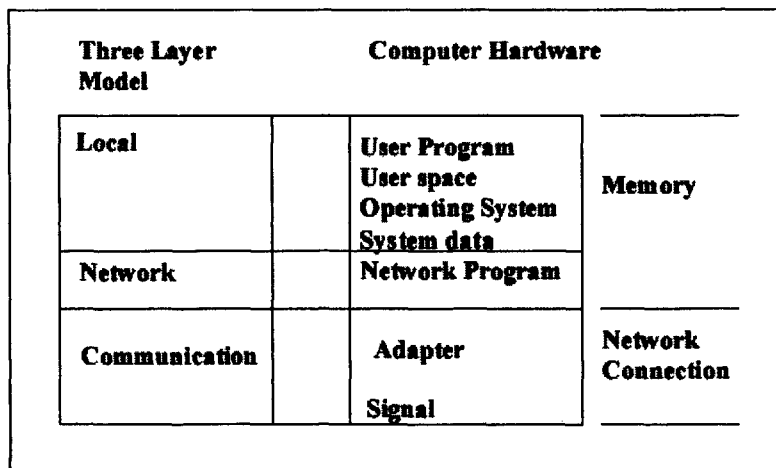


Figure 16.2 Computer hardware for three-layer model.

The local layer interfaces to the user space, local programs, and the operating system. Typically, through the operating system, connection is made to the network program, in which the network layer resides. At this point, the data then physically passes to the communication layer (See Figure 16.2) by going through the network adapter (variously called network interface card, or controller). This physically converts the data to a signal.

In a more abstract sense, Figure 16.3 shows hierarchical relationship between the three layers and the transformation that the data packet undergoes in each layer. If we begin with the sending function, the local layer identifies the data to be transmitted and formats them into a unit that contains data only. The local layer may perform operations such as encryption of the data, or transformation of the data into a way that is known by the receiver so that they can be applied to their appropriate use. The network layer appends part of the header of the packet. The information contained therein may be the length of the data, the destination address, and the sender's address.

The data and network header then physically transfers to the communication layer. This layer appends still another header (the link header), which contains synchronizing patterns, source and destination addresses and packet length. This layer also provides error-correcting information, which is usually appended as a trailer to the packet.

Packet data communication requires the distinction between the source and destination, and the intermediate destinations in routing the packet to its destination. An important assumption is that the communications layer performs the routing, and it is done between two adjacent workstations. The network layer performs the end-to-end communication, and it is between the sender and receiver. Data is left intact until the packet reaches its destination.

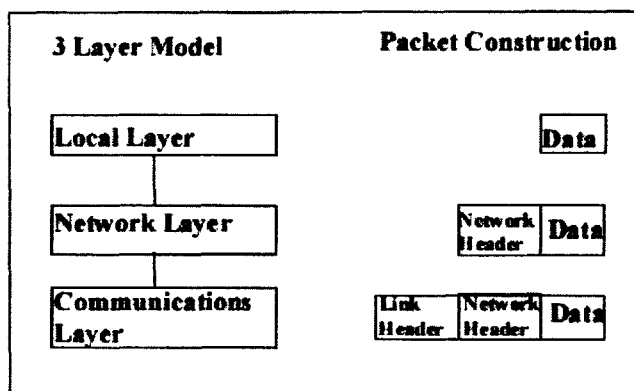


Figure 16.3 Packet construction of three-layer model.

THE OPERATION OF A COMPUTER NETWORK

To get down to the level of operation of computer networking, we can idealize the computer as shown in Figure 16.4. The computer consists of the central processing unit (CPU), memory unit, and peripheral controller to provide keyboard and other access to the outside world, and finally, storage to represent archival storage within the system. Also shown, is the network interface card (NIC), which we have labeled adapter.

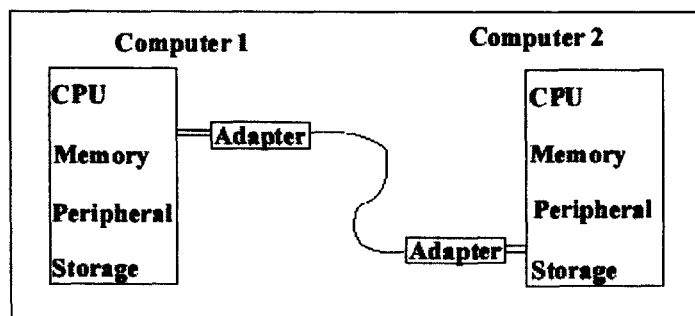


Figure 16.4 Network connection protocol.

The adapter transforms the data arriving from the system bus into the physical format required by the connection between the controllers. This connection may implement Ethernet, token-ring, or even optical systems.

Code to perform the send and the receive function follows this form:

```

Sender {
Send data
Set time out
Wait for acknowledgement
}

Receiver {
wait for data
If (data is in error)
Send negative acknowledgement
Else
Send acknowledgement
}

```

Since each of the two workstations has a sender and receiver, the interaction between them takes place to transfer data. This example is a little misleading because there is no address requirement. As long as two machines are connected together, they can interact whenever they choose. However, the addition of three or more machines requires that each machine have a unique address. This way the controller can examine the destination of each packet and accept those packets intended for its workstation.

TCP/IP

The Internet Protocol (IP) is the commonly used Internet protocol to assure the transfer of a packet from router to router. The best way to understand the capabilities available in IP is to look at the IP version for packet header. The structure follows that similar to C programming language.

IP Packet Header [

Nibble	IP version #, header length
Byte	type of service (no longer in use)
Word	packet length note that the length of the packet is limited to 64K
Word	fragmentation identifier
Nibble	flags the number of fragments to follow
Offset	the offset of this specific fragment in the message

Byte	time to live	
Byte	protocol whether TCP or UDP or other protocols	
Check sum	check sum calculated from the IP header	
Double word		source address
Double word		destination address
Double word		options (and padding)
Data]		

Very quickly we see the source and destination addresses. The fragmentation and re-assembly word that allows the packet to traverse different networks whose packet length may differ. Thus, the packet may start out as a 64K Byte packet, but an Ethernet network will truncate it to less than 1500 Bytes. These smaller packets, then, must be re-assembled at the destination to form the appropriate full-length packets.

The end-to-end message sending in an Internet system is handled by TCP, the transport control protocol. This has two issues: one, the way that the packet is sent, and two, the reconstruction of the message.

TCP is a connection-oriented datagram transmission system, so it must establish the communication path before transmitting. Establishing that path uses the TCP three-way handshake as follows. The sender requests a connection, the receiver grants the connection, the sender acknowledges the grant, thus, establishing the connection.

TCP provides what is referred to as congestion control. It does so by granting permission by means of the window protocol. In its simplest form, the window protocol allows the sender to send the number of packets up to the size of the window. Suppose window size is 8, we allow the sender to send 8 packets. The sender cannot send any more packets until it receives an acknowledgement for all 8 packets. Now we introduce an interesting problem. That is, how do we count the next set of packets? While in practice, the maximum size of the window can be substantial. In this example, we'll assume it is 8. Thus, the next packet to be sent would be 0. How do we know that it is not the original 0 packet? Because, acknowledgement for the first zeroed packet has been received by the sender, and need not be considered further.

In operation, TCP begins data transmission using the slow start: TCP sends exponentially increasing numbers of packets, beginning with one until it reaches the windows size. Each exponentially growing set is allowed to continue as long as it receives the acknowledgement from the sender. Once the acceptable window size has been received, the receiver maintains the window size.

When a sender error such as a time out occurs, the receiver senses such a timeout because the sender re-transmits the same packets. At this point, the receiver shuts down and requires the sender to re-transmit beginning again with the slow start and going up to one-half the size of the previous maximum window size, thus effecting congestion control.

Quite clearly, a determined offender can defeat the TCP/IP system by requiring the receiver to continuously shut down its window forcing congestion on the system. In addition, changing the default settings on the packet header fields can cause substantial changes in the operation of the networking system. Address spoofing is a typical example.

Future revisions of IP promise to have multicasting, the ability to broadcast to a defined group of workstations. This will make life easier for the determined intruder. Mitigating this is the promise that a more secure standard will be forthcoming. As the technology changes, the need to maintain security will unfortunately mitigate improvements in addressability and connectivity.

QUEUING AND NETWORK DELAYS

Here we develop the queuing delay equations and show how delays arise from propagation transmission and waiting in the workstation (largely due to queuing). Excessive queuing can lead to buffer overloading and possible loss of packets.

Because the derivation is based on an infinite queue, delay increases without bounds. But in the finite queue, we note that packets gets lost and more realistically mimics the true case. Unfortunately network traffic is statistically self-similar, so the problem is worse because the standard deviation cannot be counted upon to decrease, as in the Markovian-only case.

In communicating between two machines, as described above, transmission of the data takes place in unknown ways. What is important is the sending and receiving machine. In this way, the delay of transmission between the two machines, t_d , is shown in Equation 1.

$$t_d = t_p + t_t + t_w \quad (1)$$

The time delay of propagation, t_p , is given by the speed of light in the transmission medium. The delay due to transmission, t_t , is the time that the controller takes up in placing the data in the transmission medium. Typically, this is the data length divided by the data transmission rate.

The workstation delay, t_w , is in many cases an ignored, but fundamentally important component of the delay in the system. The components of the workstation delay are shown in Equation 2.

$$t_w = t_i + t_o + t_q \quad (2)$$

The instruction delay, t_i , consists of the time required to complete the currently executing instruction, plus the time required to access the interrupt service routine, and the time required to return from the interrupt service routine. Typi-

cally at this point, control is transferred to the operating system to respond appropriately to the data available at the computer. This operating system time, t_o , can be substantial, on the order of 100s of microseconds.

Finally, there is the queuing delay, t_q . This is the time required to wait in the network interface card queue until something useful can be done with the arrival packet. An opportunity for mischief comes in as a result of increasing transmission delay due to inadequate bandwidth, increasing queuing delay due to an overloading of traffic, and deadlocking the buffers.

A *queue* is a collection of objects in which each object enters, stays for a while, and leaves (See Figure 16.5). The *arrival rate* is the rate at which the object arrives in the queue. The time of arrival is randomly distributed. We usually deal with the mean arrival rate λ in objects (or elements) per second.

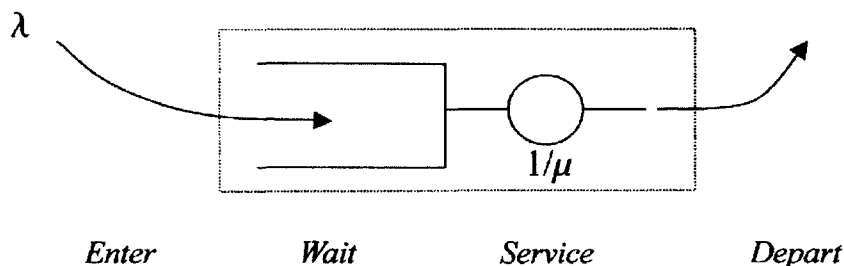


Figure 16.5 The queuing system of an object.

The duration of stay in the queue depends upon the *service time* of the server. Each object in the queue waits as long as it needs until it gets service. It waits until all objects in front of it are served, then it is allocated a specific service time. Mostly we deal with the average service time $1/\mu$ in seconds per object. After the object gets service it departs the queue.

The traditional way to model the queue makes use of Markoff chains in which each state of the chain is equivalent to the number of people in the queue. Figure 16.6 shows such a chain.

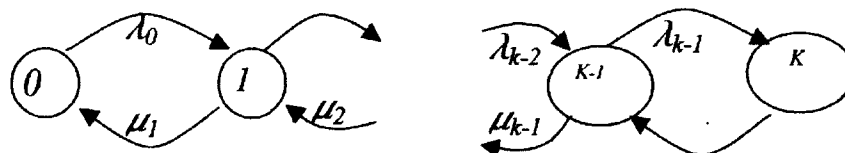


Figure 16.6 A Markoff chain for the queuing system.

Initially, in state 0, there are 0 people in the queue, and the probability with which the system goes to state 1 is $p_0\mu_0$. This is called the probability flow and is the probability of being in state 0 times the arrival rate from state 0 to state 1. Similarly, the probability flow that returns to state 0 from state 1 is $p_1\mu_1$ and is the probability of being in state 1 multiplied by service rate of the queue. That is, the arrival rate increases the number of customers in the queue while the service rate of the queue decreases the number of customers in the queue. The queue increases by 1 customer at a time until it gets to state K. Thus, one of the important assumptions is that one and only one customer enters the queue at a time. And one, and only one, customer is serviced and departs the queue at a time.

In the steady state, that is after the queue has passed through its transient phases, the queue remains stationary and it is said to be stationary in the steady state. At this point, we can solve for the probability of being in the k th state, and we can solve for that in terms of all of the previous succeeding states. Let us show how this is done.

First, we cut through the probability flows between state 0 and state 1, then the probability of flow from state 0 to state 1 is equal to the probability of the flow from state 1 to state 0. This follows because the chain is in equilibrium. Furthermore we solve for the p_1 , the probability of being in state 1

$$p_0\lambda_0 = p_1\mu_1$$

$$p_1 = \frac{\lambda_0}{\mu_1} p_0$$

Similarly, the cut between state 1 and state 2 and equilibrium allows us to equate the probability of flows from state 1 to state 2 and the return.

$$p_1\lambda_1 = p_2\mu_2$$

$$p_2 = \frac{\lambda_1}{\mu_2} p_1$$

$$= \frac{\lambda_0}{\mu_1} \frac{\lambda_1}{\mu_2} p_0$$

We have also used the previously solved value of p_1 , so that the only unknown that remains is the probability of being in state 0, p_0 , the empty state. We assume that we know the arrival and departure rates of each state.

We repeat this up to state k , cut between state $k-1$ and k , and equate the flows. We make a further simplifying assumption, and that is to make all arrivals and departures independent of state. This has the effect of removing the subscripts on λ and μ .

We solve for each p_k and substitute the previous values of λ and μ , and arrive at an expression of products of λ and μ with again the only unknown being p_0 .

$$p_{k-1}\lambda = p_k\mu$$

$$p_k = \frac{\lambda}{\mu} p_{k-1}$$

$$p_k = \frac{\lambda}{\mu} \frac{\lambda}{\mu} \dots \frac{\lambda}{\mu} p_0 = \left(\frac{\lambda}{\mu}\right)^k p_0$$

This gives us the probability of k customers in a queue. It remains to find the value of p_0 .

But first another simplification and that is to re-define the ratio of λ/μ to be equal to ρ , which becomes the efficiency of the queue. This is called the utilization of the queue and it is also a measure of the traffic. We will see that a theoretical and important condition for queue performance is $\rho < 1$. So we have

$$p_k = \rho^k p_0$$

The constitutional equation of probability is that the sum all of the probabilities is equal to 1, and we can therefore obtain an explicit expression for p_0 .

$$\sum_{k=0}^{\infty} p_k = 1 = \sum_k \rho^k p_0 = \frac{1}{1-\rho} p_0$$

$$p_0 = 1 - \rho$$

So that the final value of the probability of a queue in state k is

$$p_k = (1 - \rho) \rho^k$$

We again see the important role that $\rho = \lambda/\mu$ plays. It is a ratio of input rate to service rate, clearly the service rate must always be less than 1 or the queue grows

without bounds. Note the mathematical difficulties we get into if ρ is the same as or exceeds 1. The important result here is that physically the arrivals can overwhelm the service times resulting in pathological queue behavior.

So how do we use this information? We can obtain the number of customers in the queue N and the average transit time T through the queue system. We find N by taking the mean of the elements in the queue. For convenience we have substituted n for k .

$$\begin{aligned}
 N &= \sum_{n=0}^{\infty} n \cdot p_n \\
 &= \sum_{n=0}^{\infty} n \cdot \rho^n p_0 \\
 &= (1-\rho) \sum_{n=0}^{\infty} n \cdot \rho^n \text{ \textit{Aside: } } \sum_{i=0}^{\infty} i \cdot a^i = \frac{a}{(1-a)^2} \textit{ Geometric Series} \\
 &= (1-\rho) \frac{\rho}{(1-\rho)^2} \\
 &= \frac{\rho}{(1-\rho)}
 \end{aligned}$$

This result shows that N depends only on the traffic ρ . For a fixed service time we can vary the arrival rate. Thus ρ appears as arrival normalized by the service time. We can plot this and see the effect of the denominator: N increases without bounds as the traffic increases (Figure 16.7).

Now to find the average time a customer requires to wait in the queue and get service, that is the time required to traverse the queue system, T , requires an important relationship called Little's Law. *Little's Law* relates the number of elements in the system (N) to the *average total wait time* (T) in the system.

$$N = \lambda T$$

To find T , substitute N into Little's law and carry out the algebra. Note that we have also substituted for ρ . So the average wait time in the queue is the following.

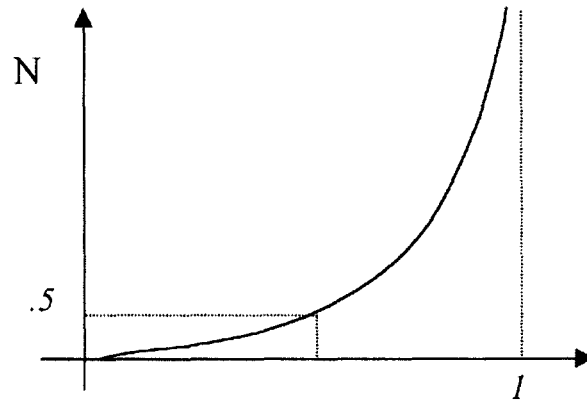


Figure 16.7 A plot of number of elements of the system (N) versus the traffic (I).

$$T = \frac{N}{\lambda} = \frac{\frac{\lambda}{\mu}}{\left(1 - \frac{\lambda}{\mu}\right)} \cdot \frac{1}{\lambda} = \frac{1}{\mu \left(1 - \frac{\lambda}{\mu}\right)} = \frac{1}{\mu - \lambda}$$

We plot T again as a function of ρ , which we can do easily since (See Figure 16.8)

$$T = \frac{1}{\mu - \lambda} = \frac{1/\mu}{1 - \rho}$$

Note that the plot again has increasing wait time with increasing traffic. There are some interesting insights that the plot will give. At a very small traffic rate the wait time is due only to the service of the queue. That is consistent with Little's Law. With no customers waiting service occurs immediately and the only delay is due to that of obtaining service. Furthermore, as the traffic rate increases the effect of waiting in the queue for service comes in. It is instructive to observe that for $\rho < 0.5$ the average number of customers is always less than one. However as ρ increases above 0.5 the number of customers in the queue increases and continues without bound up to $\rho = 1$, for an indeterminately large wait time.

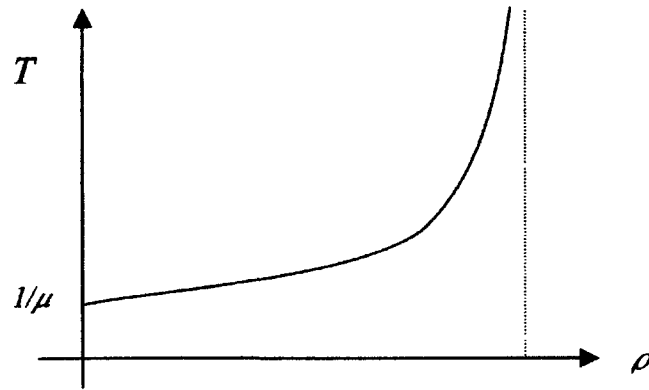


Figure 16.8 A plot of number of elements of the system (N) versus the traffic (ρ).

Now we can find other parameters describing the queue such as the wait within the queue itself, W . Figure 16.9 shows the relationship between T and W .

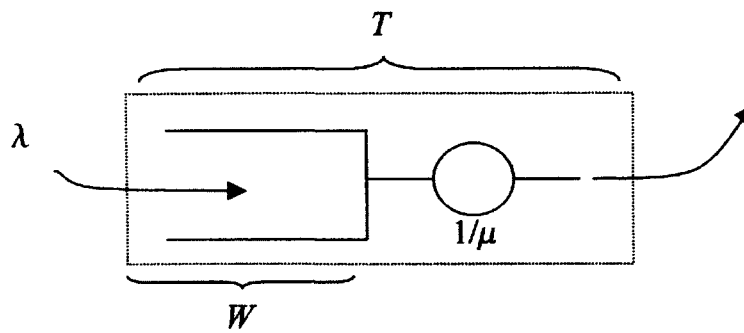


Figure 16.9 Relationship between T and W .

To find the value of W we observe that the total system wait time or the average time that a customer takes to traverse the system, is the sum of the service time and the wait in the queue as follows.

$$T = \frac{1}{\mu} + w$$

$$w = T - \frac{1}{\mu} = \frac{1}{\mu} \left(\frac{1}{1-\rho} - 1 \right) = \frac{1}{\mu} \left(\frac{\rho}{1-\rho} \right)$$

$$w = \frac{\rho}{\mu - \lambda}$$

Similarly we can find the number of customers getting service and the number of customers in the queue either by using Little's Law or by observing that the number of customers in the queue system is due to those waiting and that in service.

As the traffic increases so do the number of customers in the queue and the time to traverse the queue. This gives rise to a common technique used by cyber-terrorists—denial of service. By increasing the number of arrivals the queue size increases and the service provided to a particular customer decreases. The same effect can be gained by decreasing the service time. But in practice queues are finite. So the effect is worse, packets get lost and messages cannot be reconstructed.

A common pathology of queues is that it fills with incomplete messages, so that the queue cannot empty. A deadlock occurs in that the system cannot remove completed messages from the queue, so re-sent packets have no place in the queue and are discarded, the messages cannot be reconstructed since the packets are lost, and the queue cannot empty. In large measure the solution to this problem is obvious: empty the queue. This will be much more easily facilitated when system designers provide a "queue full" error message.

A case in point is that email queues get full when their owners do not (or cannot) empty them. One finds out that the intended recipient has a full queue when "email undeliverable" error messages return. The recipient in each case is unaware of the problem, but the sender knows well that the buffer is full.

WHAT CAN BE DONE?

Individual Computer Protection

The most common means for protection is password access. The password is intended to be a secret from all those except authorized individuals who need to use the password to gain access to the resources. The password system has been in use with computing since it was realized that it was not a good idea to give everyone access to a particular computer system.

The password system is enhanced by requiring a User ID; thus, the intruder must know both the user ID as well as the password to gain access to the system.

Let us consider the number of distinct attempts that must be tried in order to use all possible combinations of a particular password. If a password uses only one letter of the alphabet, an exhaustive attempt to by an intruder to try all the possible passwords would simply be 26, the number of letters in the alphabet. However, for two letters in the alphabet, the number of attempts is 26×26 , or the number of characters squared. Continuing on with increasing characters in the password, the general rule is that the alphabet size taken to the power of the size of the password is the number of times that is required in order for the exhaustive search of the password to be found. For example, if we allow ourselves to consider all ASCII characters (an alphabet with size 128 characters), and the password to have a width of 6, as required in many systems, the possible number of distinct passwords is

128^6 which is approximately equal to 10^{13}

Thus we see that approximately 10 trillion attempts exhaustibly tries all possible passwords. It is entirely possible that a determined intruder can gain access on the first try, or may need to wait for the last try. Thus, password searches usually attempt to use information about the user whose account is being surreptitiously accessed to reduce the number of tries.

While password access is not perfect, it is certainly useful and discouraging to most but the most determined intruders. However, associated with the password is the access privilege within the system, which means the privilege of accessing particular files or directories. It is well known in the UNIX system that privilege is granted on read, write and execute basis. Read means that the file can be opened and read; write allows modification of the file; and, finally the permission to execute the files. Each of these permissions can be granted to a file owner, who along with the super user may change the file permissions. Permissions may also be granted the system defined group, and the world, which is everybody else.

Malicious Programs

The most common way to prevent malicious programs from entering the system is to use one of the many surveillance programs available to identify viruses and other software threats in the system. Typically, the surveillance programs can be run by the user to test suspicious files, or by the system when entering new media, such as a disk, into the system. These programs require continuous updates to keep up with the variety of software threats that continue to grow.

Firewalls

With the rise of the Internet, and the implied promise of public access to a wide variety of networks, it became clear that organizations need to distinguish between private data and public data.

Furthermore, in the early days of the popular Internet, security precautions were seen not as a necessary safety feature, but as nonsense. After all, visitors were encouraged to visit the sites that were available.

The issues then of privacy and control security gave rise to firewalls to protect local networks. In essence, a firewall is a server that exists between the local site and the rest of the Internet.

An essential feature of firewall protection is that the local site can have one, and only one, entrance from the outside, and that is through the firewall. Access to any other source, whether it be telephone or a local area network, is not allowed. While there are many ways to classify firewalls, we consider only two – filter-based and proxy-based.

The filter-based firewalls are the most widely deployed type. A particularly useful filtering uses IP addresses, and TCP ports. Originating and destination addresses and ports can be filtered out, and not forwarded to their destination location.

Of course, spoofing techniques can defeat filter-based firewalls. This requires more sophisticated effort such as identifying inconsistencies in the IP address, e.g., an internal source address entering from the outside. But the primary advantage is that any data allowed into the network must first go through the firewall. Logs of activity can be maintained for an audit trail of suspicious activity.

Proxy-based firewalls provide a separation from the external client to the local server. The firewall itself acts as a server, which caches the incoming packets. The server can analyze the message for suitability. For example, a request authorized to access a private area may have a different URL from a request that has no such authority. Such information is not available from a simple examination of IP addresses.

SECURITY AND ENCRYPTION

With economically valuable information traversing the networking wires of the world, some means to protect that information must be implemented. There is substantial effort to provide security measures to protect such data based on encryption techniques. The purpose of encryption is to provide several levels of protection, and assurance concerning the data. These are authorization, privacy, integrity and authentication

Authorization is the granting of access to resources. It is the ability to receive permission to use protected resources. Password protection provides authorization to machines. Furthermore, encryption techniques may also be used to establish that authorization has been granted to use a set of resources.

Privacy is the guarantee that only the sender and the receiver have access to the information. In some cases, of course, it is possible that only the sender knows the extent of the message, and the receivers only receive portions, and vice versa. Privacy is maintained by encryption.

Integrity is the assurance that the security of the message has not been compromised, and that the message itself has not been compromised. The integrity of security can be maintained primarily by the trust in the encryption system. The integrity of the message may also require also more error dictation systems as well as the trustworthiness of the encryption systems.

Authentication is the assurance that the message was sent to the intended recipient, or that the message was sent from the authorized sender. Authentication assures that the sender and receiver are true, and that the message can be trusted as being indeed sent by the sender, or received by the recipient. Authentication techniques are required to publish digital signatures, or watermarks.

Encryption is a large area of mathematics that studies the means to transform a message into a non-readable form to all but the receiver. That is encrypt the message, and allow the receiver to convert the message back to its original state. In terms of encryption vocabulary, the original message is referred to as plain text, which gets converted to encrypted text, which in turn is decrypted back to the plain text. Of the many systems that are in use today, there are two that we will discuss. The first is called data encryption standard (DES), and the second one is referred to as RSA, after the authors of the technique.

DES, the data encryption standard, reorders the characters in the message, and substitutes new characters for the original characters. The algorithm for reordering and substitution is maintained in what is referred to as a key. Because the key expresses the algorithm, the key must be kept secret. This technique is referred to as private key encryption, and requires the same key for encryption and decryption. Thus, a fundamental weakness of this encryption standard is the need for maintaining private keys. In operation, DES has a 64-bit plain text block, and uses a 64-bit encryption key to produce the encrypted text. Within the encryption key, there are three transpositions, and 16 substitutions. Operation of the system requires the encryption algorithm, the decryption algorithm, and the key. The trustworthiness of such systems can be brought into serious question. In the early part of World War II the German encoding system, which was primarily a reorder and substitution system, was broken by the British, and used throughout the war to decode German messages.

In contrast, the RSA system is a public key system. The public key is provided to all who need to have access. That is, it is made public for the purposes of encrypting a message. It cannot be used to decrypt the message. The decryption key is not derivable from the encryption key and is kept private. It is also referred to as the secret key. Thus, only the recipient can decrypt the message. Not even the sender can decrypt the encrypted message.

The RSA technique uses the computational cost of factoring large prime numbers to create the encrypted message. Factoring large numbers is computa-

tionally expensive and factoring the message without the key is exponentially more expensive than with the key. The decryption requires a substantial algorithm and is 2 to 3 times slower than DES.

REFERENCES

1. N Wiener. Cybernetics, second edition, MIT press, 1961
2. Stock Broker. People magazine. pp 158, Nov. 9, 2000
3. DE Denning. Cyber-terrorism. <http://www.cs.georgetown.edu/~denning>.
4. MM Pollit. Cyber-terrorism-Fact or Fancy? <http://www.cs.georgetown.edu/~denning>.
5. DE Denning. Activism, Hackactivism, and Cyber-terrorism: The Internet as a tool for influencing Foreign Policy. <http://www.nautilus.org/info-policy/workshop/papers/denning.html>.

BIBLIOGRAPHY

Networking

LL Peterson, BS Davie. Computer Networks, A systems approach. 2nd Edition, Morgan Kaufmann Publishers, San Francisco, 2000.

Kurose JF and Ross KW, Computer Networking Addison Wesley, Boston, 2001.
Queueing Theory

Kleinrock L. Queueing Theory Vol 1, Chap. 6, John Wiley and Sons, New York, 1975.

Bolch G, Greiner S, de Meer H, and Trivedi KS, Queueing Networks and Markov Chains, John Wiley and Sons, New York, 1998.

Security

Scientific American 279(4): 95-117, Oct 1998.

Stallings W, Cryptography and network Security, 2nd Edition, Prentice Hall, 1998.

17

Chemical Agents: Classification, Synthesis and Properties

Dabir S. Viswanath and Tushar K. Ghosh

University of Missouri, Columbia, Missouri

CLASSIFICATION

The word, *chemical*, itself creates uneasiness, if not total fear, but the combination of the words “chemicals” and “terrorism” can be deadly. Chemical terrorism is attack on human life and destruction of property using chemicals. Chemicals used for this purpose can temporarily incapacitate and/or kill human beings, destroy property or do all at the same time. Many chemicals serve both useful and destructive purposes. A chemical used for chemical terrorism is defined as a chemical substance that could be ‘employed’ because of its direct toxic effect on humans, animals and plants. A toxic chemical can be defined as any chemical which through its chemical reaction on living processes, may cause death, temporary loss of performance, or permanent injury to people, animals or plants. The term ‘employed’ means that the chemical is dispersed or transported to the site where this toxic effect is created. Various types of ammunition and equipment has been designed for their dispersal. The Chemical Weapons Convention (CWC), Article 2, paragraph 1 defines “chemical weapons” as [1]:

1. “Chemical Weapons” means the following, together or separately:
 - (a) Toxic chemicals and their precursors, except where intended for purposes not prohibited under this Convention, as long as the types and quantities are consistent with such purposes;

- (b) Munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in subparagraph (a), which would be released as a result of the employment of such munitions and devices;
- (c) Any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (b).

The word "plants" is not specifically used in the above definition. However, the UN document on the definition of chemical warfare and toxic chemicals published in 1969 defines chemical warfare agents as "chemical substances, whether gaseous, liquid or solid, which might be employed because of their direct toxic effects on man, animals and plants". It is appropriate to include plants because chemicals can be used to destroy crops, which may lead to economic loss, fear, and panic among the general population.

Several chemicals that can be used for a terrorist attack are commercial chemicals or intermediates. It is well known that a chemical explosive, such as trinitrotoluene (TNT or dynamite) can be used for blasting off obstacles when building bridges or to bring down old buildings, but at the same time it can be used for destructive purposes. We have witnessed the destructive power of ammonium nitrate and fuel oil (both of them are available commercially) in the bombing of the Federal Building in Oklahoma City on April 19, 1995. It not only killed innocent people but also destroyed property. Such terrorist attacks can also bring down the morale of the people and loss of trust in their government. On March 20, 1995 in the Tokyo subway system two persons boarded different trains in Tokyo's main lines between 8:09 and 8:13 a.m., and planted packages, plastic containers filled with sarin and wrapped in newspapers. These containers were punctured with a needle-tipped umbrella. Twelve persons lost their lives, over 5,500 were injured, and more than 26 stations were closed. More than anything, this incident produced a tremendous psychological effect on the people of Japan, and made them think that such attacks in other parts of the country may occur and many lost confidence in the government's ability to protect its citizens.

Chemical weapons, warfare agents, or simply chemicals used in terrorist activities can be broadly classified as follows.

- Choking agents (Asphyxiating)
- Blood agents or systemic poisons
- Blister agents (Vesicants)
- Nerve agents
- Incapacitating agents
- Penetrating agents
- Tear agents (Lacrimators)
- Vomiting agents (Sternutators)
- Defoliants, Desiccants, Soil Sterilants, and Plant Growth Inhibitors.

Emerging agents

A list of these agents is given in Table 17.1. The two-letter code name (e.g., GA=Tabun) of these agents are also given in this table. The two-letter code name is mainly used to identify the agents and it has nothing to do with the chemical formula or the chemical properties of the agent. Several of these agents can persist in the environment for a longer periods of time and can cause secondary contamination if proper protection is not taken. In Table 17.1, the persistence data for these agents are given at two temperatures. Most of these agents will eventually degrade in the environment; however, as discussed in Chapter 20, most of these chemical agents can be destroyed by heating.

Choking agents

These chemicals irritate eyes and throat, and when inhaled, can lead to pulmonary edema, resulting in death from lack of oxygen. Phosgene and chlorine are classified as choking agents. Phosgene has a number of industrial uses in manufacturing various commercial products. Phosgene hydrolyses rapidly, and is used in the production of compact discs, lightweight eyeglasses, and shatterproof glasses. These products are made from polycarbonate resin, which is synthesized from phosgene that is used as a monomer in the synthesis steps. Foams, paints, fibers, and adhesives are made from polyurethanes, in which the diisocyanate monomers are made using phosgene. Phosgene is also used in making isocyanate intermediates used in the manufacture of pharmaceuticals and agricultural chemicals.

Blood agents

These are cyanide compounds, the principal one being hydrogen cyanide. Hydrogen cyanide is a colorless liquid that boils at 26°C. The main exposure route is through inhalation. Both gaseous and liquid hydrogen cyanide, as well as cyanide salts in solution, can be harmful and absorbed through the skin. Cyanide compounds are more toxic than phosgene, but evaporate very fast making them difficult to use in warfare since there are problems in achieving sufficiently high concentrations outdoors. However, the concentration of hydrogen cyanide may rapidly reach lethal levels if it is released in confined spaces making it a potent agent for terrorism.

Blister agents

These are chemicals that can cause blistering of the skin and extreme irritation of the eyes and lungs. These chemicals incapacitate rather than kill human beings but can kill in large doses. The basic agent is mustard gas. It was extensively used during World War I. Mustard gas is diphosgene, and causes shortness

Table 17.1 Chemical warfare agents that can also be used for chemical terrorism.

Type	Name	Code	Chemical Formula	Persistence 70-90 °F (hrs)	Persistence 40-60 °F (hrs)	Action
<i>Choking</i>	Phosgene	CG	COCl_2	0.5	1	Rapid
	Diphosgene	DP	$\text{C}_2\text{Cl}_4\text{O}_2$	0.5 - 3	1 - 4	Rapid
	Tabun	GA	$\text{C}_2\text{H}_5\text{OPO}(\text{CN})\text{N}(\text{CH}_3)_2$	24 - 48	48 - 96	Very rapid
	Sarin	GB	$\text{CH}_3\text{PO}(\text{F})\text{OCH}(\text{CH}_3)_2$	0.5 - 24	24 - 36	Very rapid
	Soman	GD	$\text{CH}_3\text{PO}(\text{F})\text{OCH}(\text{CH}_3)\text{C}(\text{CH}_3)_3$	24 - 48	48 - 96	Very rapid
	VX	VX	$(\text{C}_2\text{H}_5\text{O})(\text{CH}_3\text{O})\text{P}(\text{O})\text{S}(\text{C}_2\text{H}_4\text{N})(\text{C}_2\text{H}_2(\text{CH}_3)_2)_2$	240 - 720	720 - 2160	Rapid
<i>Blood</i>	Hydrogen cyanide	AC	HCN	0.25 - .5	0.5 - 1	Very rapid
	Cyanogen chloride	CK	CNCl	0.25 - .5	0.5 - 1	Rapid
<i>Blister</i>	Arsine	SA	AsH_3	0.08 - .25	0.25 - .5	Delayed
	Distilled mustard	HD	$(\text{ClCH}_2\text{CH}_2)_2\text{S}$	24 - 48	48 - 96	Delayed
	Nitrogen mustard	HN-1	$(\text{ClCH}_2\text{CH}_2)_2\text{NC}_2\text{H}_5$	24 - 48	48 - 96	Delayed
	Nitrogen mustard	HN-2	$(\text{ClCH}_2\text{CH}_2)_2\text{NCH}_3$	24 - 36	48 - 72	Delayed
	Nitrogen mustard	HN-3	$\text{N}(\text{CH}_2\text{CH}_2\text{Cl})_3$	48 - 72	96 - 144	Delayed
	Phosgene oxime	CX	CCl_2NOH	2 to 4	3 to 6	Immediate
Mustard lewisite	Lewisite	L	ClCHCHAsCl_2	18 - 36	48 - 72	Rapid
	Mustard lewisite	HL		24 - 36	48 - 72	Delayed
	Ethylidichloroarsine	ED	$\text{C}_2\text{H}_5\text{AsCl}_2$	1 to 2	2 to 3	Immediate

Table 17.1 continued

Type	Name	Code	Chemical Formula	Persistence 70-90 °F (hrs)	Persistence 40- 60 °F (hrs)	Action
<i>Blister</i>	Methyldichloroarsine	MD	CH ₃ AsCl ₂	2 to 4	4 to 8	Rapid
<i>Vomiting</i>	Diphenyl- dichloroarsine	DA	(C ₆ H ₅) ₂ AsCl	1 to 2	2 to 4	Very rapid
	Adamsite	DM	C ₆ H ₄ (AsCl)-NH)C ₆ H ₄	1 to 2	2 to 4	Very rapid
	Diphenylcyanoarsine	DC	(C ₆ H ₅) ₂ AsCN	1 to 2	2 to 4	Very rapid
<i>Riot</i>	Chloroacetophenome	CN	C ₆ H ₅ COCH ₃ Cl	1 to 2	2 to 3	Instant
	Chloroacetophenome in chloroform	CNC		1 to 2	2 to 3	Instant
	Chloroacetophenome and chloropicrin in chloroform	CNS		1 to 2	2 to 3	Instant
	Chloroacetophenome in benzene and carbon tetrachloride	CNB		1 to 2	2 to 3	Instant
	Bromobenzylcyanide	CA	BrC ₆ H ₄ CH ₂ CN	24 - 48	48 - 96	Instant
	O-chloro-benzyl- malononitrile	CS	ClC ₆ H ₄ CHC(CN) ₂	168 - 336	168 - 336	Instant
<i>Incapacitating</i>	Bz	BZ		240 - 480	720 -1440	Delayed

Source: <http://www.fas.org/nuke/guide/intro/cw/chem-table.htm>

of breath (lung irritant), nausea and blindness. Later a number of modifications were made to mustard gas to make it more toxic and lethal. These are nitrogen mustard and Lewisite. They undergo slow hydrolysis making them more persistent in the environment and in any fluid.

Nerve Agents

Nerve agents are the most poisonous synthetic chemicals, and they inhibit the vital enzyme activity, specifically of cholinesterase, which is essential for the proper functioning of the nervous system. They disrupt the normal functioning of the nervous system. All nerve agents belong chemically to the group of organophosphorus compounds. They are stable and easily dispersed and have rapid effects both when absorbed through the skin and via respiration. For example, vapor from 3 drops of a nerve agent can kill a person in 4 minutes.

Incapacitating Agents

Several chemicals in smaller doses can incapacitate a human being for a short time. Incapacitating agents are usually defined as chemical agents that produce reversible disturbances in the central nervous system that disrupt cognitive ability. The agent BZ, which was used by the military in the past but now is used in pharmacology where it is known as QNB, is a cholinergic blocking compound and produces many effects similar to those of atropine, such as mydriasis, drying of secretions, heart rate changes, and decreased intestinal motility. BZ at high doses can lead to confusion, disorientation, and disturbances in perception (delusions, hallucinations) and expressive function (slurred speech) within an hour of exposure. These symptoms are similar to high doses of atropine.

Tear Agents (Lacrimators)

These chemicals cause tears in the eyes and irritation to the skin. They can also be harmful to the respiratory tract. Even in low concentrations, they cause pain in the eyes and flow of tears and make it difficult to keep the eyes open. These substances are chloroacetophenone (CN), ortho-chlorobenzylidene-malonitrile (CS) and dibenz (b,f)-1,4-oxazepine (CR). The agent CN was the most widely used tear gas; however, recently it has been replaced by CS. At present CS is probably used most widely worldwide as tear gas for riot control. At room temperature, these tear gases are white solid substances. They are stable when heated and have low vapor pressure. Consequently, they are generally dispersed as aerosols.

Vomiting Agents (Sternutators)

As the name indicates, they cause nausea and vomiting. They can also induce cough, headache, and nose and throat irritation. Adamsite (DM) is the most common vomiting agent. It is normally a solid, but upon heating, it first vaporizes and then condenses to form aerosols. Adamsite is dispersed as an aerosol. Under

field conditions, vomiting agents can cause great discomfort to the victims. However, indoors, they can cause serious illness or death. Symptoms include irritation of eyes and mucous membranes, coughing, sneezing, severe headache, acute pain and tightness in the chest, nausea, and vomiting. DM has been noted to cause necrosis of corneal epithelium in humans. The human body will detoxify the effects of mild exposures within 30 minutes of evacuation. Severe exposures may take several hours to detoxify and minor sensory disturbances may persist for up to one day.

Defoliants, Desiccants, Soil Sterilants, and Plant Growth Inhibitors

Although we will not discuss the compounds in this category, it is important to note that these chemicals can be used for terrorist activities indirectly. Agent Orange used in Vietnam is an example. They can destroy crops, reduce the fertility of the soil, remove water from the soil and inhibit plant growth.

Emerging Agents

Many chemicals are considered out of date, and some countries are always on the lookout for more toxic chemicals. The ability to synthesize these chemicals has increased due to better communications through the Internet, enhanced computer modeling, advances in synthetic organic chemistry, and various political considerations.

Table 17.2 shows a list of toxic chemicals and precursors designated as chemical warfare agents by the Chemical Weapons Convention (CWC). They are listed under three categories: Schedule 1, 2 and 3 based on the level of their toxicity. The following guideline has been recommended by the CWC in defining a schedule category for a chemical [1].

Guidelines for Schedule 1

1. The following criteria shall be taken into account in considering whether a toxic chemical or precursor should be included in Schedule 1:
 - (a) It has been developed, produced, stockpiled or used as a chemical weapon as defined in Article II;
 - (b) It poses otherwise a high risk to the object and purpose of this Convention by virtue of its high potential for use in activities prohibited under this Convention because one or more of the following conditions are met:
 - (i) It possesses a chemical structure closely related to that of other toxic chemicals listed in Schedule 1, and has, or can be expected to have, comparable properties;

- (ii) It possesses such lethal or incapacitating toxicity as well as other properties that would enable it to be used as a chemical weapon;
 - (iii) It may be used as a precursor in the final single technological stage of production of a toxic chemical listed in Schedule 1, regardless of whether this stage takes place in facilities, in munitions or elsewhere;
- (c) It has little or no use for purposes not prohibited under this Convention.

Guidelines for Schedule 2

2. The following criteria shall be taken into account in considering whether a toxic chemical not listed in Schedule 1 or a precursor to a Schedule 1 chemical or to a chemical listed in Schedule 2, part A, should be included in Schedule 2:
- (a) It poses a significant risk to the object and purpose of this Convention because it possesses such lethal or incapacitating toxicity as well as other properties that could enable it to be used as a chemical weapon;
 - (b) It may be used as a precursor in one of the chemical reactions at the final stage of formation of a chemical listed in Schedule 1 or Schedule 2, part A;
 - (c) It poses a significant risk to the object and purpose of this Convention by virtue of its importance in the production of a chemical listed in Schedule 1 or Schedule 2, part A;
 - (d) It is not produced in large commercial quantities for purposes not prohibited under this Convention.

Guidelines for Schedule 3

3. The following criteria shall be taken into account in considering whether a toxic chemical or precursor, not listed in other Schedules, should be included in Schedule 3:
- (a) It has been produced, stockpiled or used as a chemical weapon;
 - (b) It poses otherwise a risk to the object and purpose of this Convention because it possesses such lethal or incapacitating toxicity as well as other properties that might enable it to be used as a chemical weapon;

- (c) It poses a risk to the object and purpose of this Convention by virtue of its importance in the production of one or more chemicals listed in Schedule 1 or Schedule 2, part B;
- (d) It may be produced in large commercial quantities for purposes not prohibited under this Convention.

In Table 17.2 numbers in square brackets show the CAS (Chemical Abstracts Service) Registry numbers, a unique way of identifying chemical substances. There is no significance to these numbers, but are an unambiguous computer-language description of a compound's molecular structure. A precursor is a chemical that can be chemically combined with another substance to form a chemical substance – in this case a chemical warfare agent. Many precursors are controlled through international efforts but have other commercial uses as well. Therefore it is possible to obtain these precursors and use them to make toxic chemicals.

Table 17.2 List of toxic chemicals and precursors.

Schedule 1

A. Toxic chemicals

O-Alkyl (less than or equal to C₁₀, incl. cycloalkyl) alkyl (Me, Et, n-Pr or i-Pr)-phosphonofluoridates

Sarin: O-Isopropyl methylphosphonofluoridate [107-44-8]

Soman: O-Pinacolyl methylphosphonofluoridate [96-64-0]

O-Alkyl (less than or equal to C₁₀, incl. cycloalkyl) N, N-dialkyl (Me, Et, n-Pr or i-Pr) phosphoramidocyanidates

Tabun: O-Ethyl N, N-dimethylphosphoramidocyanidate [77-81-6]

O-Alkyl (H or less than or equal to C₁₀, incl. cycloalkyl) S-2-dialkyl (Me, Et, n-Pr or i-Pr)-aminoethyl alkyl (Me, Et, n-Pr or i-Pr) phosphonothiolates and corresponding alkylated or protonated salts

VX: O-Ethyl S-2-diisopropylaminoethylmethyl phosphonothiolate [50782-69-9]

Sulfur mustards

2-Chloroethylchloromethylsulfide [2625-76-5]

Mustard gas

Bis(2-chloroethyl)sulfide [505-60-2]

Bis(2-chloroethylthio)methane [63869-13-6]

Sesquimustard

1,2-Bis(2-chloroethylthio)ethane [3563-36-8]

1,3-Bis(2-chloroethylthio)-n-propane [63905-10-2]

Table 17.2 (continued)

Sesquimustard (continued)

1,4-Bis(2-chloroethylthio)-n-butane [142868-93-7]

1,5-Bis(2-chloroethylthio)-n-pentane [142868-94-8]

Bis(2-chloroethylthiomethyl)ether [63918-90-1]

O-Mustard

Bis(2-chloroethylthioethyl)ether [63918-89-8]

Lewisites

Lewisite 1: 2-Chlorovinylchloroarsine [541-25-3]

Lewisite 2: Bis(2-chlorovinyl)chloroarsine [40334-69-8]

Lewisite 3: Tris(2-chlorovinyl)arsine [40334-70-1]

Nitrogen mustards

HN1: Bis(2-chloroethyl)ethylamine [538-07-8]

HN2: Bis(2-chloroethyl)methylamine [51-75-2]

HN3: Tris(2-chloroethyl)amine [555-77-1]

Saxitoxin [35523-89-8]

Ricin [9009-86-3]

B. Precursors

Alkyl (Me, Et, n-Pr or i-Pr) phosphoryldifluorides

DF: Methylphosphoryldifluoride [676-99-3]

O-Alkyl (H or less than or equal to C₁₀, incl. cycloalkyl) O-2-dialkyl (Me, Et, n-Pr or i-Pr)-aminoethyl alkyl (Me, Et, N-Pr or i-Pr) phosphonites and corresponding alkylated or protonated salts

QL: O-Ethyl O-2-diisopropylaminoethylmethylphosphonite [57856-11-8]

Chlorosarin

O-Isopropyl methylphosphonochloridate [1445-76-7]

Chlorosoman

O-Pinacolyl methylphosphonochloridate [7040-57-5]

Table 17.2 (continued)**Schedule 2****A. Toxic chemicals**

Amiton:

O,O-Diethyl S-[2-(diethylamino)ethyl] phosphorothiolate [78-53-5] and corresponding alkylated or protonated salts

PFIB:

1,1,3,3,3-Pentafluoro-2-(trifluoromethyl)-1-propene [382-21-8]

BZ:

3-Quinuclidinyl benzilate [6581-06-2]

B. Precursors

Chemicals, except for those listed in Schedule 1, containing a phosphorus atom to which is bonded one methyl, ethyl or propyl (normal or iso) group but not further carbon atoms e.g., Methylphosphonyl dichloride [676-97-1]

Dimethyl methylphosphonate [756-79-6]

Exemption

Fonofos:

O-Ethyl S-phenyl ethylphosphonothiothionate [944-22-9]

N,N-Dialkyl (Me, Et, n-Pr or i-Pr) phosphoramidic dihalides

Dialkyl (Me, Et, n-Pr or i-Pr) N,N-dialkyl (Me, Et, n-Pr or i-Pr)-phosphoramidates

Arsenic trichloride [7784-34-1]

2,2-Diphenyl-2-hydroxyacetic acid [76-93-7]

Quinuclidine-3-ol [1619-34-7]

N,N-Dialkyl (Me, Et, n-Pr or i-Pr) aminoethyl-2-chlorides and corresponding protonated salts

N,N-Dialkyl (Me, Et, n-Pr or i-Pr) aminoethane-2-ols and corresponding protonated salts

N,N-Dimethylaminoethanol [108-01-0] and corresponding protonated salts

N,N-Diethylaminoethanol [100-37-8] and corresponding protonated salts

N,N-Dialkyl (Me, Et, n-Pr or i-Pr) aminoethane-2-thiols and corresponding protonated salts

Thiodiglycol: Bis(2-hydroxyethyl)sulfide [111-48-8]

Pinacolyl alcohol: 3,3-Dimethylbutane-2-ol [464-07-3]

Table 17.2 (continued)**Schedule 3****A. Toxic chemicals**

- Phosgene: Carbonyl dichloride [75-44-5]
- Cyanogen chloride [506-77-4] (2851.00)
- Hydrogen cyanide [74-90-8] (2811.19)
- Chloropicrin: Trichloronitromethane [76-06-2]

B. Precursors

- Phosphorus oxychloride [10025-87-3]
- Phosphorus trichloride [7719-12-2]
- Phosphorus pentachloride [10026-13-8]
- Trimethyl phosphite [121-45-9]
- Triethyl phosphite [122-52-1]
- Dimethyl phosphite [868-85-9]
- Diethyl phosphite [762-04-9]
- Sulfur monochloride [10025-67-9]
- Sulfur dichloride [10545-99-0]
- Thionyl chloride [7719-09-7]
- Ethyldiethanolamine [139-87-7]
- Methyldiethanolamine [105-59-9]
- Triethanolamine [102-71-6]

Source: Organisation for the Prohibition of Chemical Weapon (OPCW), 2001. <http://www.opcw.org/>. [2].

SYNTHESIS

In this section we will discuss the synthesis steps of a few representative chemicals. The manufacturing facilities generally required are available to any country with a good chemical industry infrastructure. The major equipment required in all cases include mainly reaction vessels, agitators as most of the manufacturing is carried out in a batch process, heat exchangers or condensers, pumps, valves, storage tanks, controllers and measuring equipment (for measuring temperature, pressure or vacuum, toxic gas detectors, flow meters, etc.), balances, and analytical equipment. In all cases, materials of construction are important, as most of the chemicals handled are highly corrosive. Some materials of construction

used in these plants are glass-lined vessels, tantalum, graphite, titanium, zirconium, and alloys of some of these metals. The materials of construction are expensive items in the manufacture of these toxic chemicals.

Many chemicals like phosgene and hydrogen cyanide can be procured directly, as they have several commercial uses. Toxic chemicals like mustard gas (most of the vesicants) can be prepared easily, and the technology is well known. Nerve gas is more complicated to synthesize, and in many cases fairly precise control of variables such as temperature is required. These chemicals need more sophisticated technologies. Of the several nerve gases, Tabun, O-ethyl dimethylamidophosphoryl cyanide, GA, is the easiest to manufacture. Most advanced countries think that tabun is out-of-date, and look for other nerve gases. We shall now take specific cases and outline the synthesis procedure.

Mustard

Bis(2-chloroethyl)sulfide, a heavy oily liquid, is made by Levinstein process. It consists of bubbling dry ethylene into sulfur monochloride at 35°C with previously prepared mustard facilitating the reaction. The reaction is



The nitrogen mustards are a series of chloroalkyl amines, the most active being tris(2-chloroethyl)amine $[\text{N}(\text{C}_2\text{H}_4\text{Cl})_3]$ and methyl-bis(2-chloroethyl)amine $[\text{CH}_3\text{N}(\text{C}_2\text{H}_4\text{Cl})_2]$. These nitrogen mustards are highly active vesicants. The nitrogen mustards are prepared by the reaction of thionyl chloride with the appropriate ethanolamine.



Sarin

Sarin $[\text{C}_4\text{H}_{10}\text{FO}_2\text{P}]$ is methylphosphorofluoridic acid 1-methylethyl ester or isopropylmethane-fluorophosphonate. Its Chemical Abstracts Service registry number is 107-44-8. It was discovered in 1938 by Gerhard Schrader, the German chemist, during World War II, but fortunately was not used. It is an organophosphate, a class of chemicals used as pesticides, and it was during the synthesis of pesticides that sarin was accidentally discovered. These organophosphates are highly toxic and stable. It has been replaced by other substances such as VX Sarin, one of most deadly compounds in the weapons arsenal. Closely related to sarin is a compound referred to as GF, or cyclohexyl sarin. GF is also a colorless and odorless liquid.

Large-scale combat use of sarin has not occurred, although its use is strongly suspected in an Iraqi attack on the village of Birjinni on 25 August 1988 (samples collected from the site four years later showed the expected breakdown products of sarin). It is not known with certainty whether or not sarin was used in

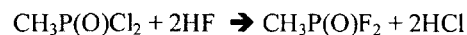
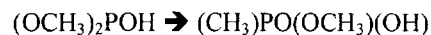
the Iran-Iraq war. On 20 March 1995, the Aum Shinrikyo released sarin in the Tokyo subway, killing 12 and injuring 5,500 people in the first documented terrorist use of chemical weapons. Sarin was produced and stockpiled in large quantities by both the United States and the Soviet Union.

Reesor et al. [3] discuss several routes for the synthesis of sarin. According to Reesor et al., the direct conversion of phosphorous trichloride to methylphosphonic dichloride, and its subsequent conversion to sarin is a safer method. The formation of aluminum phosphorous chloride or modified APC is the first step in the process. The dichloride is converted into difluoride, and finally to sarin.

A second route for isopropyl methylphosphanofluoridate, is the reaction of dicyclohexylamine salt of *o*-isopropyl hydrogen methylphosphonothioate with picryl fluoride [4]. Both Reesor et al. and Boter and Van Den Berg [4] describe the experimental details for the preparation of alkyl methylphosphonofluoridates.

On method that is followed in the manufacture of sarin is the DHMP (Dimethyl hydrogen phosphite) process although other processes have replaced this process. In the DHMP process, phosphorous trichloride and methanol are reacted to give dimethyl phosphite. On further heating, dimethyl phosphite is converted to methyl phosphonate. This mixture called "pyromix" is chlorinated using chlorine and phosphorous trichloride to yield methylphosphonic dichloride. This is then fluorinated to yield the difluoride, which combines with dichloride to yield sarin.

During the different stages corrosive and toxic chemicals such as HCl, methyl chloride, oxychloride and others are formed. The last stage can take place in missiles during flight, as the reactants are far less dangerous than the product so that they can be stored separately. The reaction scheme is shown below as an illustrative example [5].



PROPERTIES OF CHEMICALS

Knowledge of the properties of chemicals is important to measure the effectiveness of chemical compounds. We will discuss some simple properties and how they can tell us the effectiveness of chemical compounds. Various physical and chemical properties of chemical agents are given in Table 17.3.

Table 17.3 Physical and chemical properties of chemical agents.

Agent	MW	State @ 20°C	Odor	Liquid Density (g/cc)	BP (°C)	VP (mmHg)	Volatility (mg/m ³)	ΔH_v (cal/g)
Tabun	162.3	Colorless to brown liquid	Faintly fruity; none when pure	1.073 ^{25°C}	240	0.037 ^{20°C}	610 ^{25°C}	79.56
Sarin	140.1	Colorless liquid	Almost none when pure	4.86	158	2.9 ^{25°C} 2.10 ^{20°C}	22,000 ^{25°C} 16,090 ^{20°C}	80
Soman	182.18	Colorless liquid	Fruity; cam- phor when impure	1.022 ^{25°C}	198	0.4 ^{25°C}	3,900 ^{25°C}	72.4
Cyclo-sarin	180.2	Liquid	Sweet; musty; peaches; shellac	1.133 ^{20°C}	239	0.044 ^{20°C}	438 ^{20°C}	90.5
VX	267.38	Colorless to amber liquid	None	1.0083 ^{20°C}	298	0.0007 ^{20°C}	10.5 ^{25°C}	78.2 ^{25°C}
V _x	211.2	Colorless liquid	None	1.062 ^{20°C}	256	0.007 ^{25°C} 0.004 ^{20°C}	75 ^{25°C} 48 ^{20°C}	67.2
Distilled Mustard HD	159.08	Colorless to pale yel- low liquid	Garlic or horseradish	1.27 ^{25°C} 1.27 ^{20°C}	217	0.072 ^{20°C}	610 ^{20°C}	94

MW: Molecular weight; BP: Boiling point; ΔH_v : Heat of vaporization

Table 17.3 continued

Agent	MW	State @ 20°C	Odor	Liquid Density (g/cc)	BP (°C)	VP (mmHg)	Volatility (mg/m ³)	ΔH _v (cal/g)
Nitrogen Mustard HN-1	170.08	Dark liquid	Fishy or musty	1.09 ^{20°C}	194	0.24 ^{25°C}	1,520 ^{20°C}	77
Nitrogen Mustard HN-2	156.07	Dark liquid	Soapy (low concentra- tions) Fruity (high)	1.15 ^{20°C}	75 at 15 mmHg	0.29 ^{20°C}	3,580 ^{25°C}	78.8
Nitrogen Mustard HN-3	204.54	Dark liquid	None, if pure	1.24 ^{20°C}	256	0.0109 ^{25°C}	121 ^{25°C}	74
Phosgene oximedi- chloro- foroxime	113.94	Colorless solid or liquid	Sharp, pene- trating	—	53–54 at 28 mmHg	11.2 ^{25°C} (solid) 13 ^{40°C} (liquid)	1,800 ^{20°C}	101 at 40°C
Lewisite	207.35	Colorless to brownish	Varies; may resemble ge- raniums	1.89 ^{20°C}	190	0.394 ^{20°C}	4,480 ^{20°C}	58 at 0°C to 190°C
Mustard- Lewisite mixture	186.4	Dark, oily liquid	Garlic	1.66 ^{20°C}	<190	0.248 ^{20°C}	2,730 ^{20°C}	58 to 94

MW: Molecular weight; BP: Boiling point; ΔH_v: Heat of vaporization

Table 17.3 continued

Agent	MW	State @ 20°C	Odor	Liquid Density (g/cc)	BP (°C)	VP (mmHg)	Volatility (mg/m ³)	ΔH _v (cal/g)
Phenyl dichlorarsine	222.91	Colorless liquid	None	1.65 ^{20°C}	252 to 255	0.033 ^{25°C}	390 ^{25°C}	69
Ethyl dichlorarsine	174.88	Colorless liquid	Fruity, but biting; irritating	1.66 ^{20°C}	156	2.09 ^{20°C}	20,000 ^{20°C}	52.5
Methyl dichlorarsine	160.86	Colorless liquid	None	1.836 ^{20°C}	133	7.76 ^{20°C}	74,900 ^{20°C}	49
Hydrogen cyanide	27.02	Colorless gas or liquid	Bitter almonds	0.687 ^{20°C}	25.7	742 ^{25°C} 612 ^{20°C}	1,080,000 ^{25°C}	233
Cyanogen chloride	61.48	Colorless gas or liquid	Pungent, biting; Can go unnoticed	1.18 ^{20°C}	12.8	1,000 ^{25°C}	2,600,000 ^{20°C}	103
Arsine	77.93	Colorless gas	Mild garlic	1.34 ^{20°C}	-62.5	11,100 ^{20°C}	30,900,000 ^{20°C}	53.7 ^{-62.5°C}
Phosgene	98.92	Colorless gas	New-mown hay; green corn	1.37 ^{20°C}	7.6	1.173 ^{20°C}	4,300,000 ^{7.6°C}	59
Diphosgene	197.85	Colorless gas	New-mown hay; green corn	1.65 ^{20°C}	127 – 128	4.2 ^{20°C}	45,000 ^{20°C}	57.4

MW: Molecular weight; BP: Boiling point; ΔH_v: Heat of vaporization

Table 17.3 continued

Agent	MW	State @ 20°C	Odor	Liquid Density (g/cc)	BP (°C)	VP (mmHg)	Volatility (mg/m ³)	ΔH _v (cal/g)
Diphenyl chloroarsine	264.5	White to brown solid	None	1.387 ^{50°C}	333	0.0036 ^{45°C}	48 ^{45°C}	56.6
Adamsite	277.57	Yellow to green solid	None	1.65 ^{20°C} (solid)	410	Negligible	Negligible	80
Deiphenyleyanoarsine;	255.0	White to pink solid	Bitter almond-garlic mixture	1.334 ^{35°C}	350	0.0002 ^{20°C}	2.8 ^{20°C}	71.1
BZ	337.4	White crystal	None	1.33	320	0.03 ^{70°C}	0.5 ^{70°C}	62.9
Chloroacetophenone;	154.59	Solid	Apple blossoms	1.318 ^{20°C} (solid)	248	0.0041 ^{20°C}	34.3 ^{20°C}	98
Chloroacetophenone in Chloroform;	128.17	Liquid	Chloroform	1.40 ^{20°C}	60 to 247	127 ^{20°C}	n/a	n/a
Chloroacetophenone and Chloropicrin in Chloroform	141.78	Liquid	Flypaper	2	60 to 247	78 ^{20°C}	610,000 ^{20°C} (includes solvent)	n/a

MW: Molecular weight; BP: Boiling point; ΔH_v: Heat of vaporization

Table 17.3 continued

Agent	MW	State @ 20°C	Odor	Liquid Density (g/cc)	BP (°C)	VP (mmHg)	Volatility (mg/m ³)	ΔH _v (cal/g)
Chloroacetophenone in Benzene and Carbon Tetrachloride	119.7	Liquid	Benzene	1.14 ^{20°C}	75 to 247	variable; mostly solvent vapor	n/a	n/a
Bromobenzylcyanide	196	Yellow or solid liquid	Soured fruit	1.47 ^{25°C}	Decomposes at 242	0.011 ^{20°C}	115 ^{20°C}	79.5 ^{20°C}
O-chlorobenzyl malonitrile	188.5	Colorless solid	Pepper	1.04 ^{20°C}	310 to 315	0.00034 ^{20°C}	0.71 ^{25°C}	53.6
CR	195.25	Yellow powder in solution	Burning sensation	---	335	0.00059 ^{20°C}	0.63 ^{25°C}	---
Chloropicrin	164.38	Liquid	Stinging; pungent	1.66	112	18.3 ^{20°C}	165,000 ^{20°C}	---

MW: Molecular weight; BP: Boiling point; ΔH_v: Heat of vaporization

Molecular Weight

Molecular weight is found by adding the atomic weights of all the elements in that compound. Molecular weight can provide the following important information regarding a chemical:

Stability: Higher molecular weight compounds are less stable compared to lower molecular weight. A stable compound persists in the environment for a longer period of time compared to an unstable compound.

Protection: Gas masks and other equipment are used for protection. Based on molecular weight, higher molecular weight materials can be filtered more easily compared to lower molecular weight materials. For example it is difficult to adsorb substances like Co and ammonia using activated carbon filters. We should of course, hasten to add that filtration of the materials depends on the properties of the filtering material.

Estimation of unknown properties: Molecular weight helps to estimate unknown properties to a fair amount of accuracy. For example if we wish to find the boiling point of a substance, we can plot boiling points of some known substances of similar chemical nature and extrapolate or interpolate to get the boiling point using the molecular weight of the substance in question.

Boiling Point

Boiling point is the temperature at which a substance boils at 1.013 bar pressure. This temperature is termed as the normal boiling point. Boiling point tells us the ability of a compound to vaporize and therefore the evaporation rates. Higher boiling compounds are less volatile compared to lower boiling compounds. Therefore higher boiling compounds persist longer compared to lower boiling compounds. An estimate of the boiling point also throws some light on the rate of decontamination.

Density

Density is defined as Mass/Volume. It is the mass of a substance contained in a unit volume. It is found by weighing a known volume of the substance at a particular temperature, and dividing the mass by the volume. It is generally expressed as gm/cc or gm/cm³. When this number is compared to the density of water, the number is called specific gravity. We say that the specific gravity of mercury is 13.6, and this indicates that mercury is 13.6 times heavier than to water.

Liquid density is a measure of the effectiveness of a chemical substance as toxicity is expressed in terms of units of mass. The chemical efficiency of a munition is defined as

$$\mu = \text{mass of the filling/total mass of the munition.}$$

Therefore a chemical of a higher density has a higher efficiency for a given mass of the munition. Densities are also useful to find out whether the particular chemical floats or sinks in water. This is useful again in decontamination with water and subsequent disposal of the chemical.

Vapor Pressure

This is a very important property of the chemical. It is the pressure exerted by a liquid or a vapor when the two are in equilibrium at a particular temperature. Lower boiling substances have a higher vapor pressure and vice versa. Higher vapor pressure indicates higher evaporation rates. Chemicals therefore must have reasonable vapor pressure to be useful. Liquids and solids can be atomized and disseminated in the gaseous phase. When the toxic chemical is dispersed in the gaseous phase, the effectiveness of the chemical also depends on a number of factors such as wind speed and direction, atmospheric temperature, solar radiation, and conditions of the area such as hills, vegetation, etc.

It is very important to have knowledge of the vapor pressure at different temperatures particularly for the storage and transport of the toxicants. However the toxicity of the chemicals makes it very difficult to experimentally determine the vapor pressure at different temperatures particularly at higher temperatures. However in the range of temperature where the vapor pressure does not exceed 760 mm of Hg, vapor pressures can be estimated using the relation

$$\ln P = a + (b/T)$$

where P is the vapor pressure in mm of Hg and T is the absolute temperature in Kelvin (K). The two constants in the equation a and b can be estimated using two values of P. Table 17.4 gives the values of the constant for some specific compounds. It is recommended that these constants be used with caution, and for pressures below 760 mm of Hg.

Table 17.4 Vapor pressure constants

Chemical Compound	a	b
Tabun	21.548	-7287.4
Sarin	21.008	-5941.1

Volatility

Volatility is defined as the mass of a chemical in vapor per unit volume of air at a given temperature. Volatility depends on boiling point, vapor pressure, and temperature. It is calculated using the ideal gas equation, and is given by

$$m = 15826 P \times MW/T$$

where m is the volatility mg/m^3 , P is the vapor pressure in mm of Hg, MW is the molecular mass of the chemical, and T is the temperature in K.

This relation shows that as molecular mass increases volatility increases. However the effect of temperature and pressure are related in the sense that when the temperature increases vapor pressure increases. The increase or decrease of volatility depends on the temperature-pressure relation.

Enthalpy of Vaporization

This is the amount of heat required to vaporize a unit mass of a chemical at a given temperature and at its vapor pressure. The enthalpy of vaporization of water at 298.15 K is 540 calories per gram. This value indicates the ability of a substance to volatilize.

Advantages and Disadvantages of Chemical Weapons

Advantages

Chemical warfare agents exhibit unique qualities compared to conventional weapons. Effect of chemical weapons can be severe and rapid and have the enormous capability to inflict casualties. They may be difficult to detect at times because of their low concentrations in the environment. Effective detectors are lacking both when the substance is used and when it is stored. Also it is difficult to judge terrorists' capabilities since a number of precursor chemicals that can be used to produce chemical terrorism agents have dual use. Many chemicals can be bought or shipped as commercial chemicals. An example is thiodiglycol used in the manufacture of mustard gas, which can also be procured for making ammonium nitrate. A dedicated and skilled chemist can synthesize most these agents. With the current sophistication of computer chemical modeling, a good chemist can work out strategies for synthesizing more toxic chemicals starting from the currently available chemical structures. Compared to a nuclear weapon, the manufacturing cost for chemical agents are relatively low and in most cases require low technology.

Disadvantages

The major disadvantages are that the manufacturing processes demand good control of variables, and the chemicals are corrosive.

REFERENCES

1. Texts of the chemical weapons convention. <http://www.opcw.org/cwcdoc.htm>.

2. Preparatory Commission for the Organization for the Prohibition of Chemical Weapons PC-V/B/WP.10, February 22, 2001 <<http://www.opcw.nl/guide.htm>>.
3. JB Reesor, BJ Perry, Sherlock, E. The synthesis of highly radioactive isopropyl methylphosphonofluoridate (sarin) containing P^{32} as tracer element. *Can J Chem* 38:1416-1427, 1960.
4. HL Boter, GR Van Den Berg. Organophosphorous compounds III. *Recueil* 85: 919-927, 1966.
5. Sarin Home page. www.chem.ox.ac.uk/courses/firstyearonline/week02/sarin1.htm.
6. Air Force Manual No. 355-7, Potential Military Chemical/ Biological Agents and Compounds December 1990, Washington, D.C.1.27.

18

Chemical Agents: Toxicity and Medical Management

L. David Ormerod

University of Missouri, Columbia, Missouri

INTRODUCTION

Toxic chemicals are defined as "any chemical which, through its chemical effect on living processes, may cause death, temporary loss of performance, or permanent injury to people and animals" [1]. Industrial production since the late nineteenth century has continued to generate exponential increases in the number of toxic substances identified. Currently as many as 500,000 US commercial products pose physical or health hazards [2]. In 1999, the Environmental Protection Agency (EPA) estimated that approximately 850,000 facilities in the country were working with hazardous chemicals. Indeed, there are perennial risks of releases of hazardous materials (hazmats), because of mishaps in chemical manufacturing and storage, from industrial accidents, as a result of transportation accidents, or from accidents in the home. So far, most chemical spills are small with few casualties [3]. HAZMAT response guidelines, training, and equipment have been standardized by the National Fire Academy (NFA) and the Federal Emergency Management Agency (FEMA) in order to manage hazardous chemical accidents efficiently [4]. A newly perceived threat to the US homeland involves the deliberate use by terrorists of chemical weapons or many of these industrial chemicals against civilian populations with the purpose of maximizing casualties. As mentioned in Chapter 17 and also in Chapter 21 (Table 21.1), a number of precursors for synthesis of chemical weapons have dual use. Therefore, proliferation of these chemical agents to terrorist groups is a real possibility.

THE HAZARDS FROM CHEMICAL WEAPONS (CW)

There are three main hazards from chemical weapons: inhalational absorption; a contact hazard from skin and eye exposure; and a less frequent risk from ingestion. The methods of dissemination that might be employed are selected in accordance with the physical and chemical properties of the material to be dispensed. Chlorine and phosgene gases were the first form of mass chemical attack, but subsequent CW agents have been liquids or solids at normal temperature and atmospheric pressure. Liquids are much easier to manufacture, store, and transport than gaseous agents. Mustard and nerve gases are not gases, but are in fact liquids.

Liquid CW agents are usually dispersed as aerosols (a cloud of suspended microscopic droplets) or as vapor (the gaseous form of a substance at a temperature lower than its boiling point at a given pressure). Other methods of dissemination are as a spray or liquid to be deposited under the effect of gravity on people or surfaces, or in mixed physical form by explosive or mechanical means. Pyrotechnic dispersion is only feasible for agents with low boiling points that are heat-resistant and non-combustible. The physical properties of the CW may change during propagation if the agent evaporates or condenses. The vapors of CW are heavier than air and so will tend to concentrate under gravity into depressions, basements, etc. However, vapor and aerosol clouds have low settling velocities and the rate of deposition depends principally on chemical and physical forces that bind to specific surfaces, such as soil. The most important losses from a vapor or aerosol cloud result from low-level atmospheric turbulence.

Volatility is inversely proportional to the persistence of the CW agent. The more volatile a chemical, the more quickly it evaporates from contaminated surfaces and the greater is the danger from its vapor. There is an arbitrary division created between non-persistent chemicals that vaporize in less than 24 hours, e.g., phosgene, sarin, and hydrogen cyanide, and those with a liquid hazard persisting for longer than this threshold, e.g., mustard agent and VX. Environmental factors modify these considerations. Militarily, it was advantageous to consider non-persistent agents if it was planned for military forces to occupy the area and to use persistent agents for territory denial.

There are universal terms that provide comparative values of CW toxicity [5]. The ED_{50} and the ID_{50} denote the quantities of liquid agent exposure in μg , mg , or g quantities that will predictably cause effects (E) or incapacitation (I) in 50% of a group. The LD_{50} is the mean exposure that kills 50% of a group. Because of differences in absorption, the ED_{50} and LD_{50} are site-specific with regard to inhalational or surface exposures, and ocular absorption through the conjunctivae may sometimes be significantly greater than through dry skin surface. Comparison of the amounts of CW exposure as aerosol, vapor, or gas is achieved by use of the Concentration Time Product, or Ct. The agent concentration expressed as mg/m^3 is multiplied by the time of exposure in minutes [5]. For example a sarin Ct product of $100 \text{ mg}\cdot\text{min}/\text{m}^3$ could have resulted from a one-minute exposure at a concentration of $100 \text{ mg}/\text{m}^3$ or a four-minute exposure at $25 \text{ mg}/\text{m}^3$ and both will have

the same effects. For most CW, an approximately linear relationship is observed (Haber's Law), without accounting for differences in rates and depth of respiration, or for ill health. Several of the CW are exceptions at low concentrations when there is some metabolic detoxification of the agents. The toxicities of riot control CW are expressed as TC_{50} , the concentration that will induce a noticeable effect in 50% of exposed persons, and as the IC_{50} , that gives the concentration that is intolerable to 50% of individuals.

Such values are estimated adult values. Children and the elderly are populations at particular risk. Several factors are common to children that make them especially vulnerable [6]: higher respiration rates increase respiratory exposure; high vapor densities cause higher concentrations close to the ground; the larger surface-to-mass ratio and more permeable skin enhance systemic absorption; and the lesser degrees of keratinization in childhood skin make it more vulnerable to vesicant and corrosive agents. Other factors may compound the additional hazards to children as they may lack the cognitive and physical abilities to flee, may be difficult to isolate in personal protective devices, and, when injured, are more vulnerable to dehydration and shock as a result of vomiting and diarrheal fluid losses.

The physicochemical characteristics of the major CW agents are given in the previous chapter in Table 17.1.

ROUTES OF EXPOSURE

The lungs are usually the primary organ of exposure to CW agents, because the massive pulmonary surface area that is specialized for gaseous exchange affords the main site of poisoning, and because frequently the lungs are injured directly by the chemicals. Volatile and lipophilic agents readily cross-respiratory epithelium and obtain equilibrium concentrations in the blood. Aerosolized particles of 1 to 6 μm in diameter are retained within the lungs and continue to be absorbed even after the individual is removed from exposure. Fine particles of $<0.6\mu\text{m}$ in size will not be retained unless they are able to volatilize within the lung. Particles of size 5 to 10 μm are retained in the nose, sinuses, and throat from where they may be swallowed and add an ingestion component to the poisoning [6]. Protection from non-persistent agents is primarily with the use of respirators although skin protection is also necessary.

Skin absorption of CW for most agents is several orders of magnitude less toxic than for respired vapors, and effects are usually delayed. Many CW agents are hydrophobic, lipophilic chemicals and are readily absorbed on skin contact, especially in the moist axillary and inguinal areas. Poorly volatile persistent agents such as VX or vesicant agents are effective by contaminating the environment and clothes. In these circumstances or when equipped only with respiratory protection in areas of high vapor concentration in the immediate vicinity of a release site, skin absorption may be a primary route of poisoning. Protection from skin-active agents requires respirators, protective footwear and dermal protective clothing.

Oral ingestion can occur in contaminated water and food, by swallowing contaminated respiratory mucus, or by hand-mouth contact [7]. Alimentary poisoning leads to delayed symptoms and increased systemic effects. Particle size is immaterial to surface or gastrointestinal contamination. Toxic weapons can also be disseminated by the deliberate or incidental spiking of drinking water or food-stuffs.

If large quantities of agent are used, even a spray of widely varying droplet size will quickly produce lethal levels of vapor, while the large droplets settle onto victims or contaminating contact surfaces [8]. Highly reactive compounds such as nerve agents and cyanides penetrate and permeate through clothing and latex rubber, necessitating the manufacture of protective equipment from specialized materials. The effectivity of agents is generally greatest within confined indoor space.

ENVIRONMENTAL CONSIDERATIONS

A slight breeze of about 3 to 4 miles per hour at night, or close to dawn or dusk, is optimal for the outdoors release of CW agents. Particulate behavior within a cloud is discussed in Chapter 4. The chemical cloud passes along the axis of wind travel from a point or line release and is spread laterally by diffusion, wind shear and turbulence, and by variations in terrain that may disperse or trap the CW in depressions. The cloud layer closest to the ground travels slowest because of friction. As the density of the CW causes a tendency to settle, the cloud travels in a fashion similar to ocean waves breaking upon the shoreline [9]. Thermal activity on warm sunny days will also disrupt a CW cloud during daylight hours. The processes of evaporation and condensation occur as the cloud travels. Agents subject to hydrolysis are susceptible to degradation in wet environments, and rain will scour CW clouds, minimizing their dissemination.

Cityscapes present a confusing terrain of urban canyons in which an agent might be remarkably persistent near the ground or mixed by turbulence over extensive vertical heights between tall buildings. Road and pavement surfaces may absorb CW and be vaporized on heating. Certainly, agent fatality predictions that are generally based upon open field use are probably unreliable. Building air conditioning systems and vertical cavities such as elevator shafts and stairwells introduce novel considerations.

SIGNS SUGGESTIVE OF A CHEMICAL ATTACK

At the scene of sudden medical casualties of uncertain etiology, initial responders need to be especially alert to any signs suggestive of a CW attack. Many agents are odorless and the chemical/vapor cloud may be invisible. This decision-making is critical if first responders are not to become secondary casualties of the event. In the Aum Shinrikyo attack on the Tokyo underground utilizing relatively small amounts of low-grade sarin, at least 10% of the emergency service personnel

and medical staff became mild casualties [8,10]. A more substantial attack would undoubtedly have led to responder fatalities. If a chemical attack is suspected, it is important that first responders delay entry into the area until adequate protection is obtained.

The most significant sign is the simultaneous development of similar symptoms in a large group of people [11]. All helpers must first protect themselves before venturing further; civilians must be prevented from rushing in to rescue the victims. Other indications of a possible chemical release [11, 12] are:

- mass casualties in absence of trauma
- casualties distributed in a pattern consistent with agent dissemination
- lower attack rates in either indoors or outdoors
- unusual liquid droplets on vegetation; oily film on water
- discolored vegetation
- numerous dead animals, birds, fish
- lack of insect life; it may be easiest to determine
- insect kill on the surface of water
- exposed individuals reporting unusual odors or tastes
- reported muffled small explosions or dispersing mists
- abandoned spray devices or dispersal ordinance containing liquids
- civilian panic

ADVICE TO CIVILIANS INVOLVED IN A CHEMICAL RELEASE

The primary protection against a chemical attack upon civilians is intelligence. The sharing of intelligence with the public is justified if the risk is considered cogent as general awareness can be a potent deterrent. Certain precautions can be taken in the event of a CW attack, or of an industrial accident [9, 12].

If involved in an outdoors exposure, an attempt should be made to evacuate calmly, if possible in an upwind direction from the release site after determination of the wind direction. Hyperventilation may increase exposure. Emergency personnel may be able to provide emergency field shelters with positive pressure ventilation and CW absorptive filters. Escape in a vehicle should be made according to available directions from emergency personnel and away from residual mists, anticipating that there may be many others with the same motivation. The vehicle windows should be rolled up, the vents closed, and air conditioning/heater turned off.

If inside, and involved in an indoors chemical release, the building should be evacuated while minimizing passage through the contaminated area. Windows and doors should be kept closed. If inside and the building is in the path of an outdoors toxic cloud, people are usually best advised to stay indoors as this affords protection from CW in liquid form, and partial protection from aerosols and gases. The air conditioning and heating units must be turned off. Windows and doors should

be sealed with plastic tape or damp towels, tap water must be avoided, and sojourn established on higher floors to await instruction from rescuing authorities. The use of rubberized raincoats, boots, mittens, thick plastic sheets, etc, provides some protection against residual chemical cloud in the event of an evacuation. Baby cots and children can be covered in blankets. Eye sealing goggles and scuba gear should be worn if available. Return to the building must occur only on the advice of emergency authorities as decontamination may be necessary.

Once clear of the contaminated area, all external apparel should be removed and left outside. Immediate showering and vigorous scrubbing with soap and water should be undertaken and symptomatic individuals need to be rushed to available medical attention. All exposed individuals need to be triaged.

PROTECTION OF FIRST RESPONDERS

Local Fire Service and HAZMAT crews, emergency medical services, and police are at risk of direct contamination at the incident site, quite possibly to high concentrations of the CW. The precise nature of the chemical poisoning and the precise risks will likely not be known. Respiratory and personal protection equipment (PPE) is obligatory and a worse case scenario will usually be assumed. Traditional HAZMAT operations are based upon adjacent-site decontamination of relatively small numbers of casualties with procedures that are considerably time and labor consuming. With mass casualties, compromises will have to be made and efforts concentrated upon the most contaminated individuals before triage and transport to hospital. It is important that all emergency and decontamination data accompany patients to hospital. Decontamination, medical care, and triage are the main initial objectives. Extensive emergency decontamination facilities are also going to be required at each health care institution-receiving patients. Hospital first responders will need to be equipped with respiratory and personal protection devices. In the Tokyo subway sarin attack, 75% of the casualties made their own way to medical attention, bypassing the overburdened on-scene decontamination processes.

First responders in the field must be equipped with Level A protective gear [9, 13] to withstand high CW concentrations. A detailed discussion on PPE for CW has been provided in Chapter 22. This will entail provision of (1) a prefitted pressure-demand full-facepiece Self-contained Breathing Apparatus (SCBA) or pressure-demand supplied air respirator with escape SCBA; (2) a fully encapsulating vapor protective and chemical-resistant suit; (3) inner chemical-resistant gloves; and (4) chemical-resistant safety boots and shoes. Radio communication is necessary when wearing such protection.

Hospital first responders, including front-line hospital security, are exposed to lesser CW agent concentrations emanating from contaminated casualties and field equipment. Rapid emergency decontamination before entering the hospital facility will be necessary for all but the most severely ill who should be cordoned

in special facilities cared for by fully protected staff until resuscitation permits adequate decontamination. Less rigorous protection is required for hospital first responders, such as Level C equipment [14] comprising less expensive barrier materials and a full-facepiece, air purifying cannister-equipped respirator. Body fluids such as blood, vomitus, urine, fecal material, and tracheal aspirate have to be treated as potentially dangerous according to universal precautions.

Work in PPE equipment is arduous and prone to heat stress. Regular rest periods must be incorporated for all PPE-equipped personnel. Training in equipment use is necessary and fatalities can result from improper mask-use [15].

ORGANIZATION OF RESCUE OPERATIONS AFTER CW ATTACK

It is most likely that responsibility for initial crisis management would fall upon local emergency assets, particularly HAZMAT teams (see Chapter 24). The National Fire Academy (NFA) has adopted an incident analysis process, GEDAPER, comprising 7 steps:

- Gathering information
- Estimating course and harm
- Determining strategic goals
- Assessing tactical options and resources
- Planning and implementation of actions
- Evacuating
- Reviewing

Terrorist CW attacks may provide first responders with unique exposure risks, novel emergency management problems, potential exposures to unfamiliar dangerous chemicals, and mass casualties beyond current experience and training. The lack of official DOT or UN symbol identifiers or documentary evidence in CW terrorism is inconsistent with traditional HAZMAT experience. Current emergency planning is based upon known vulnerabilities and hazard identifications that permit reasonably accurate risk predictions, but which are absent in most terrorist CW attacks. The lack of familiarity with CW agents and their release in such low-risk locations as public gathering places present new conundra that must be recognized if first responders are to avoid secondary casualties. Hazardous materials frequently require different levels of protection and necessitate different protective equipment, skills, and operational approaches. In the absence of good indications as to the nature of the threat, the appropriate decisions may at first be unclear.

Regardless of the incident, the first step is to collect all available information as quickly as possible before going any further. A formal institutionalized discipline is operant in the emergency responder community under the leadership of an Incident Commander working within an Incident Command System [13]. Protocols call for an initial thorough assessment and analysis of the incident site from a

safe distance, with observation of the ambient conditions. The first priority is to keep all others away and to avoid approaching the victims until full protection is assured. Obtaining immediate assistance from the Regional Poison Center may assist the Incident Commander in his decision-making. Secure cordons are established to delimit the exclusion (hot) zone in which anyone leaving is assumed to be contaminated, the contamination reduction (warm) zone in which decontamination is performed, the support/clean (cold) zone, and a perimeter cordon for crowd control. The formally designated layout of work zones ensures that dirty and clean zones are understood by everyone. A safe refuge for contaminated individuals is set up to reduce the chances of secondary contamination and to set the stage for triage, decontamination, and medical treatment. Safe distances may be determined using the DOT Emergency Response Guidebook [16], by consulting a commercial reference source such as Chemtrec [17], or by using other reference sources.

DECONTAMINATION OF CASUALTIES

Precise recommendations for civilian mass casualty decontamination have yet to be established [18]. High decontamination capacity is one of the factors that may reduce the consequences of CW attack. Hospital decontamination ought to be performed away from the emergency room to prevent contamination and closure of the facility. All clothing and personnel effects must be removed outdoors, using extreme care not to transfer CW agent to the skin, and stored in labeled, sealed biohazard bags. Ideally, this should occur within the containment zone. Severely contaminated individuals must be decontaminated as a matter of extreme urgency within a matter of minutes. Immediate self-decontamination may be feasible if facilities happen to be available. Copious eye irrigation with suitable available non-toxic fluids and scrubbing with soap and water by protected attendants will remove surface contamination from most CW agents. Solutions of baking soda, mild bleach and sodium thiosulphate may hydrolyse residual CW agents [19]. Oily persistent agents may require the use of alcohol, acetone, paraffin, or other solvents. Vesicant (blister agents) contamination of hair or beard is best managed by cutting or shaving of the hair. Military forces have access to commercial decontaminants formulated for field use with specific CW types [9, 19, 20]. Pure metals and strong corrosives require dry powder decontamination and gentle brushing or vacuuming before water is applied [21]. The Water Authorities must be notified about contaminated wastewater produced by the decontamination process.

Ill individuals require concomitant decontamination and medical resuscitation and treatment. Decontamination of these individuals can be a difficult process, but must be achieved to reduce further poisoning and prevent injury to the medical staff and contamination of the facility. Dead individuals also require decontamination. Substances that have already reacted with the skin are generally inaccessible to decontamination regimens and may lead to further systemic poisoning. As-

ymptomatic individuals with perceived mild exposure might be treatable by sending the accompanied person home to take an immediate shower with scrubbing before reporting to a separate triage center away from the incident site [22, 23]. Observation holding areas may also be used.

The decontamination of equipment and the environment is a complex problem, in the preserve of the specialist. It must be appreciated that nerve and vesicant agents penetrate and permeate many different types of material such as plastics, paint, and rubber, from which the agents can be released over relatively long periods. Resistant paints and materials are used militarily. Contaminated sites may need to be cordoned off for a long period as the area is environmentally decontaminated. Building decontamination from a CW is a problem fraught with problems of public acceptance.

CHEMICAL WEAPON POISONING AND MANAGEMENT

Nerve Agents

The nerve agents are stable, soluble in water, easily dispersed, and highly toxic in liquid and vapor state by respiratory, mucosal, cutaneous, and gastrointestinal exposure. VX agent is the most toxic chemical known, other than certain toxins (see Table 18.1); as little as 1 mg can be lethal to an adult. Death is often rapid. Symptoms from the inhalation of vapor or aerosol occur within seconds or minutes of exposure. Cutaneous absorption is typically delayed from several minutes to a few hours. Thousands of tons of VX and the similar agent, VR, had been stockpiled by numerous nations by the end of the twentieth century because of their extreme toxicity and their versatility.

The nerve agents bind to the enzyme cholinesterase which is a crucial enzyme present at nerve terminals. When cholinesterase is inhibited, acetylcholine, a nerve transmitter agent active in the synaptic cleft between nerve junctions, is not broken down and therefore accumulates producing an unmodulated overstimulation. There are two kinds of acetylcholine receptors - (a) muscarinic receptors found in smooth involuntary muscle, in secretomotor fibers to secretory glands, and in the central nervous system; and (b) nicotinic receptors that are mainly distributed at the motor end plates of skeletal voluntary muscle.

The symptom complex of nerve agent toxicity [24] is somewhat variable depending on the route and rate of systemic poisoning and also varying somewhat with specific nerve agents. Knowledge of severe nerve agent poisoning in man is limited, but there are considerable data on poisonings from closely related organophosphate pesticides. Incomplete syndromes are common. Symptoms of initial poisoning include: (i) increased salivation and nasal discharge; (ii) miotic pinpoint pupils that impair night vision; (iii) blurred near vision with ocular pain; (iv) bronchospasm and respiratory distress; (v) nausea and dizziness; (vi) headache; and (vii) marked tiredness, hallucinations, and slurred speech. Greater exposures be-

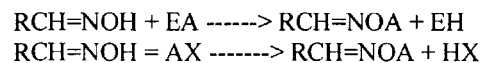
come more and more incapacitating. The symptoms of advanced nerve agent poisoning [22] include:

- intractable salivation, lacrimation, micturition, and defecation
- excessive sweating
- severe muscular weakness and tremors
- coughing, difficulty in breathing, cyanosis, and apnea
- abdominal pain, nausea and vomiting
- anxiety, confusion, convulsions, and coma

Severe poisoning of nerve agent causes pronounced muscular symptoms. Death is due to acute respiratory failure caused by central effects in the brain and from paralysis of the respiratory muscles. Oxygen supplementation should be given at an early stage. Toxicity data for the nerve agents are shown in Table 18.1 and contrasted with other CW agents.

Atropine is the principal antidote for organophosphate poisoning. It acts by binding reversibly to muscarinic acetylcholine receptors. The action of acetylcholine at these receptors is blocked militating against the increased acetylcholine receptor barrage. Atropine is given in adults at a dosage of 4 to 6 mg I/M or I/V statim, repeated in 2mg I/M or I/V increments as needed over several days - titrated against the decrease in bronchial secretion, bronchial constriction, and in improvements in blood gas analysis results. Diazepam 10mg slow I/V is given in severe poisoning for its anticonvulsant action.

Oximes, of which there are several, e.g., 2-PAM (pralidoxime) and HI-6, possess a -CH=NOH group and can (a) reactivate bound cholinesterase, and (b) bind to unbound nerve agent (A)



The combination of atropine and oxime therapy is markedly synergistic. Acetylcholinesterase bound to nerve agent can fairly rapidly become covalently bound in an irreversible process known as 'aging' - this mainly occurs with soman poisoning. The dosage of pralidoxime is 1 to 2g I/V over 5 to 20 minutes; the dose may be repeated every 4 to 6 hours until nicotinic signs resolve. Neither atropine nor pralidoxime is very effective against CNS signs. Obidoxime is the most effective oxime against tabun poisoning. The military prepares these antidote agents as autoinjectors suitable for personal emergency use. In severe cases of nerve agent poisoning, antidotal treatment will not be sufficient by itself for survival.

Ventilatory support may be required for patients with impending respiratory failure. It is likely to be required for several days until cholinesterase levels are functionally restored. A patient under optimal intensive care from the onset of symptoms may recover from doses as high as 100 times the LD₅₀. Mechanical ventilators will likely be at a premium after a major nerve agent attack.

Table 18.1 Estimated Chemical Weapon Toxicities.

Agent	Effect	Ct ₅₀ (mg .min/m ³)	Liquid on skin
<i>Nerve Agents</i>			
Tabun (GA)	miosis	~2-3	
	death	200-400	50-60 mg/kg
Sarin (GB)	miosis	~3	
	death	100-200	20-25 mg/kg
Soman (GD)	miosis	~2-3	
	death	50-70	4-5 mg/kg
VX	death	10-50	<0.1 mg/kg
Vesicant agents			
Distilled HD mustard	eye	12-200	
	pulmonary	100-200	
	erythema	200-1000	10 µg
	death	1,500 inhalation 10,000 skin	100 µg/kg
Lewisite (L)	erythema	>1,500	10-15 µg
	death	~1,500 inhalation	40-50 mg/kg
Phosgene (CX) oxime	eye	(?) 200	
	erythema	(?) 2,500	
	death	(?) 3,200	
<i>Choking Agents</i>			
Phosgene (CG)	pulmonary	>1,600	
	death	3,200	
<i>Blood Agents</i>			
Hydrogen (AC) cyanide	death	2,500-5,000	
	Cyanogen (CK) chloride	death	11,000

Source: Adapted from USAMRICD Medical Management of Chemical Casualties Handbook, 2000.

Carbamates can be used as a prophylactic pretreatment. Carbamylated acetylcholinesterase cannot combine with the nerve agent and hydrolysis slowly restores the native enzyme. Pyridostigmine can be kept up on a 30mg 8-hourly schedule for several days aimed at protecting about a third of the blood cholinesterase; it is stopped immediately if poisoning occurs. Partial brain cholinesterase protection can be established prophylactically using a combination of two centrally acting drugs, the carbamate, physostigmine, and the anticholinergic, scopolamine. This is mainly a military usage.

Vesicating (Blistering) Agents

These blistering and tissue-injuring agents are highly reactive, persistent compounds that combine with numerous biological molecules, notably acting as alkylating agents. These agents can cause severe damage to the lungs, eyes, skin, and other tissues. The two main groups of vesicants are the mustards and the dichlorarsine derivatives. All the mustards contain at least two 2-chloroethyl groups, attached either to thioether residues (sulfur mustards) or to amine residues (nitrogen mustards).

Although mustard agent is readily soluble in organic solvents, it is only minimally soluble in water, in which it slowly hydrolyses. Sulfur mustard is another CW that readily crosses the skin and mucous membranes; it interacts with the skin and causes significant tissue damage over a wide range of exposures.

Decontamination later than a minute or two following exposure, will reduce but not prevent skin damage. Neutralizing chemicals such as chloramine solutions or neutral absorbing powders, such as Fuller's earth, may be available. No clinical effects at all are observed for a 2 to 24 hour latent period. When the contaminating incident is not noticed, timely decontamination is infeasible. Progressive ocular irritation with tearing, photophobia, and blepharospasm are noticed first, followed by a dusky skin erythema, productive cough, and hoarseness. Extensive skin blistering, hyperpigmentation, and scarring may follow with delayed healing over many weeks. Skin injuries are more severe in humid and hot climatic conditions.

This agent is a potent cause of chronic disability. The ocular and pulmonary complications are particularly serious and severely poisoned individuals may develop pulmonary edema and chemical pneumonia that can lead to chronic, fibrotic, bronchiectatic lung disease [23]. Respiratory involvement is indicated by a persistent nonproductive cough, shortness of breath, and hoarseness. Scarred, vascularized corneas and severe dry eyes can be a long-term consequence causing blindness in severely affected individuals. An ill-understood syndrome of chronic ocular surface inflammation many years after the attack may occur.

Alimentary absorption causes severe, acute gastrointestinal damage with nausea and vomiting and massive fluid losses. Fluid losses from these chemical burns are relatively small unlike those experienced in thermal injuries and fluid overload should be avoided. A prolonged leucopenia and pancytopenia is rela-

tively common in severe poisoning and is a factor in the development of complicating life-threatening infective complications. It requires therapy with granulocyte, platelet, and blood transfusions. Two to three percent of military victims die because of severe pulmonary disease, death generally occurring a week or two after the attack.

The most important affect of these agents is their considerable long-term morbidity. There is no therapy for mustard poisoning other than decontamination and supportive measures that include wound dressings, with regimens similar to third-degree thermal burn care, and pulmonary management with antibiotics, bronchodilators, intubation, and assisted ventilation. Ocular lubricating ointments and limited topical corticosteroid therapy, sometimes assisted with tectonic surgery and late corneal grafting, are used to help ameliorate the eye damage. Plastic surgery may be required for late cicatricial skin changes.

Lewisite and phosgene oxime cause similar lesions to the mustard agents. However, both cause immediate ocular and skin pain and respiratory symptoms on contact with vapor, so that detection and immediate decontamination are much more likely. They produce a similar clinical picture to mustard agents. Eye lesions may be particularly serious. British Anti-Lewisite (BAL: dimercaprol) is an antidote of moderate effectivity in early poisoning by these agents. BAL treatment consists of 3mg/kg dosage 4-hourly for 2 days, then 2mg/kg 12-hourly for the next 10 days, varied with body size and disease severity. BAL can also be applied to the eyes and skin if preparations are available. Neither agent damages lymphoid tissues.

Blood Agents (Cyanides)

Hydrogen cyanide and cyanogen chloride are volatile liquids that cause death by interfering with metal-containing enzymes, notably the cytochrome oxidases involved in tissue respiration and energy generation. The most likely route of poisoning is by inhalation. Liquid and aerosols also penetrate skin readily and induce irritation, and is also absorbed from the gut.

Non-specific findings, such as headache, weakness, restlessness and a feeling of throat constriction characterize sublethal exposures. A high venous pO_2 relative to arterial pO_2 should raise clinical suspicion of the diagnosis, as tissues are unable to utilize oxygen. As severe poisoning develops, there is a brief period of rasping hyperventilation, rapidly followed by convulsions, respiratory failure, apnea, and cardiac arrhythmias, and death. Cyanosis is notably absent. Hyperbaric oxygen therapy can be used, if available. Promptness of diagnosis of symptomatic individuals and intervention are critical. Victims who remain asymptomatic several minutes after removal from known cyanide vapor require no oxygen or antidotes. Decontamination of clothing and equipment is unnecessary because of the high volatility of these agents, whose vapor is lighter than air.

Supplementary oxygen at high dosage is given. The detoxification of cyanide [25, 26] can be enhanced by intravenous 25% sodium thiosulfate that con-

verts cyanide to thiocyanate. A temporary sequestration of cyanide can be achieved by using the high binding affinity of ferric ions in methemoglobin to bind to cyanide: intravenous 3% sodium nitrate or dimethylaminophenol (DMAP) are used to temporarily produce methemoglobinemia. Intravenous hydroxycobalamin (vitamin B12) can also be used to bind cyanide and is then excreted in the urine.

The effects of cyanogen chloride are similar and its systemic toxicity is due to its conversion to hydrogen cyanide in the body. Cyanogen chloride is particularly irritating to the eyes. These agents are highly volatile and lethal concentrations are difficult to achieve unless released into a confined space.

Choking Agents (Lung Irritants)

Chlorine, phosgene, chloropicrin, and perfluoroisobutylene (a pyrolysis product of Teflon 7) are volatile liquids that cause damage at different levels within the lung. Chlorine principally damages the upper respiratory tract, trachea, and larger bronchi, chloropicrin tends to affect the medium and small bronchi, and phosgene acts directly on the alveolar-capillary membrane barriers in the lung. Exposure to all these agents can lead to acute pulmonary edema, and common secondary infection. Shortness of breath and a persistent productive cough begin within 4 to 24 hours of exposure; exertion will worsen toxicity. The ocular and skin surfaces are irritated at concentrations as low as 3 parts per million. After the initial symptomatic period, there may be a variable period in which the symptoms improve or disappear, before the development of pulmonary edema, hypoxia, and hypercarbia. Chest X-rays may show diffuse infiltration of the lung fields. Death may occur from pulmonary failure or from laryngeal spasm. Long exposures to low levels mainly cause pulmonary edema. Effects of exposure may be delayed, and asymptomatic individuals need to be observed for the development of pulmonary edema over 48 hours.

Decontamination is urgent. There is no antidote and management is supportive with oxygen, bronchodilators, oral corticosteroid, and sometimes with intubation and pulmonary ventilation. In most victims, the clinical signs of pulmonary edema, abnormal blood gases, and reduced measures of lung permeability settle within a week. However, chronic lung damage may be a consequence of severe poisoning. Shortness of breath, asthma, and reduced physical activity may persist in some for the remainder of their lives.

Phosgene release is seen commonly in building fires as a product of the pyrolysis of chlorinated plastics used in construction materials and furnishings [6]. Chloropicrin is a powerful irritant to the skin and eyes and can result in permanent scarring, especially on contact. Persistent nausea, vomiting, colic, and diarrhea may occur with heavy poisoning.

Psychotomimetic Agents

Chemicals that induce incapacitating mental changes similar to psychotic episodes, which are relatively transitory, and disable decision-making might have value to a terrorist organization. BZ produces a condition similar to atropine poisoning with dry mouth, bounding palpitations, large mydriatic pupils, impaired near vision, confusion, hallucinations, and coma. Phencyclidine causes disturbed body awareness and vivid dreams. LSD is markedly hallucinogenic. Aerosol inhalation is the most likely route of exposure.

Toxin Agents

By convention, toxins are considered biologically-produced substances and their control is incorporated in the Biological and Toxic Weapon Convention (BWTC), even if synthetic. A few toxins are the most poisonous substances known and in behavior resemble hazardous chemicals. The most important differences are the poor volatility and lack of skin penetration [27]. Toxins are generally more difficult to produce in large quantities than CW and many are unstable in aerosols. Botulinum toxin is the most poisonous substance known and can be weaponized as an aerosol. It is 1,500 more toxic than VX agent and causes death through paralysis of the respiratory muscles; mechanical ventilation may be required for many weeks or months. Emergency botulinum antiserum and therapy with the diaminopyridines may be helpful

Other toxins of interest include saxitoxin (paralysis), ricin (cardiac failure), staphylococcal enterotoxin (gastrointestinal and systemic effects), and certain snake venom toxins. There are presently few specific therapeutic interventions for toxin effects. The many classes of toxins and differing mechanisms of action would make identification and management of toxin exposures problematic. The trichothecane mycotoxins and microcystin are unusual in being dermally active. Rifampin protects against microcystin-induced liver damage in animals.

The poor volatility of most toxins means that they would pose neither significant environmental threat nor persist on skin or clothing, making protective clothing and elaborate decontamination less important. They are also more readily removed from the air by air-conditioning systems. Another difference is that many toxins are immunogenic and potentially neutralizable by appropriate vaccines; this is more applicable to prophylactic military protection. Toxin detection generally requires very sensitive assays as the most potent agents would need to be present in only very small amounts.

There are valuable treatises [5, 7, 28, 29] on the features and management of chemical weapon poisoning which should be consulted whenever a thorough treatment of the subject is desired. A summary of major CW agents and toxins is given in Table 18.2.

Table 18.2 Some potential chemical terrorism agents and syndromes (including biological toxins).

Agents	Symptom Onset	Symptoms	Signs	Clinical Diagnostic Tests	Decontamination	Exposure Route and Treatment (adult dosages)	Differential diagnostic considerations
Nerve agents	Vapors: seconds Liquid: minutes to hours	Moderate exposure: Diffuse muscle cramping, runny nose, difficulty breathing, eye pain, dimming of vision, sweating. High exposure: The above plus sudden loss of consciousness, flaccid paralysis, seizures	Pinpoint pupils (miosis) Hyper-salivation Diarrhea Seizures	Red blood cell or serum cholinesterase (whole blood) Treat for signs and symptoms: lab tests only for later confirmation Collect urine for later confirmation and dose estimation	Rapid disrobing Water wash with soap and shampoo	Inhalation & dermal absorption Atropine (2 mg) iv or im (titrate to effect up to 6 to 15 mg) 2-PAMCI 600 mg injection or 1.0 g infusion over 20-30 minutes. Additional doses of atropine and 2-PAMCI depending on severity. Diazepan or lorazepam to prevent seizures if >4 mg atropine given ventilation support.	Pesticide poisoning from organophosphorous agents and carbamates cause virtually identical syndromes

Table 18.2 Continued.

Agents	Symptom Onset	Symptoms	Signs	Clinical Diagnostic Tests	Decontamination	Exposure Route and Treatment (adult dosages)	Differential diagnostic considerations
Cyanide	Seconds to minutes	<p>Moderate exposure: Dizziness, nausea, headache, eye irritation</p> <p>High exposure: Loss of consciousness</p>	<p>Moderate exposure: non-specific findingd</p> <p>High exposure: Convulsions, cessation of respiration</p>	<p>Cyanide (blood) or thiocyanate (blood or urine) levels in lab.</p> <p>Treat for signs and symptoms: lab tests only for later confirmation</p>	Clothing removal	<p>Inhalation & dermal absorption</p> <p>Oxygen (face mask)</p> <p>Amyl nitrite</p> <p>Sodium nitrite (300 mg iv) and sodium thiosulfate (12.5 g iv)</p>	<p>Similar CNS illness results from: carbon monoxide (from gas or diesel engine exhaust fumes in closed spaces)</p> <p>H₂S (sewer, waste, industrial sources)</p>
Blister agents	2-48 hours	<p>Burning, itching, or red skin</p> <p>Mucosal irritation (prominent tearing, and burning and redness of eyes)</p> <p>Shortness of breath</p> <p>Nausea and vomiting</p>	<p>Skin erythema</p> <p>Blistering</p> <p>Upper airway sloughing</p> <p>Pulmonary edema</p> <p>Diffuse metabolic failure</p>	<p>Often smell of garlic, horseradish, and mustard on body</p> <p>Oily droplets on skin from ambient sources</p> <p>No specific diagnostic tests</p>	<p>Clothing removal</p> <p>Large amounts of water</p>	<p>Inhalation & Dermal absorption</p> <p>Thermal burn type treatment</p> <p>Supportive care for Lewisite/Mustard mixture: British Anti-Lewisite (BAL or Dimer-caprol)</p>	<p>Diffuse skin exposure with irritants, such as caustic, sodium hydroxide (NaOH) from trucking accidents</p>

Table 18.2 Continued.

Agents	Symptom Onset	Symptoms	Signs	Clinical Diagnostic Tests	Decontamination	Exposure Route and Treatment (adult dosages)	Differential diagnostic considerations
Pulmonary agents (phosgene)	1-24 hours (rarely up to 72 hours)	Shortness of breath Chest tightness Wheezing Mucosal and dermal irritation and redness	Pulmonary edema with some mucosal irritation (more water solubility = more mucosal irritation)	No tests available but source assessment may help identify exposure characteristics (majority of trucking incidents generating exposures to humans have labels on vehicle)	None usually needed	Inhalation Supportive care Specific treatment depends on agents	Inhalation exposures are the single most common form of industrial agent exposure (e.g. HCl, Cl ₂ , NH ₃) Mucosal irritation, airways reactions, and deep lung effects depend on the specific agent especially water solubility
Ricin (castor bean toxin)	18-24 hours	Ingestion: nausea, diarrhea, vomiting, fever, abdominal pain Inhalation: chest tightness, coughing, weakness, nausea, fever	Clusters of acute lung or GI injury; circulatory collapse and shock	ELISA (from commercial laboratories) using respiratory secretions serum and direct tissue	Clothing removal Water rinse	Inhalation & Ingestion Supportive care for ingestion: charcoal lavage.	Tularemia, plague, and Q fever may cause similar syndromes, as many CW agents such as Staphylococcal enterotoxin B and phosgene

Table 18.2 Continued.

Agents	Symptom Onset	Symptoms	Signs	Clinical Diagnostic Tests	Decontamination	Exposure Route and Treatment (adult dosages)	Differential diagnostic considerations
T-2 myco toxins	2-4 hours	Dermal & mucosal irritation, blistering and necrosis Blurred vision, eye irritation Nausea, vomiting and diarrhea Ataxia Coughing and dyspnea	Mucosal erythema and hemorrhage Red skin, blistering Tearing, salivation Pulmonary edema Seizures and coma	ELISA from commercial laboratories Gas chromatography/Mass spectroscopy in specialized laboratories	Clothing removal Water rinse	Inhalation & dermal contact Supportive care For ingestion: charcoal lavage Possibly high dose periods	Pulmonary toxins (O ₃ , NO _x , phosgene, NH ₃) may cause similar syndromes though with less mucosal irritation

Source: Office of Public Health and Environmental Hazards and Department of Veterans Affairs.

LONG-TERM CONSEQUENCES OF CW EXPOSURE

Long-term sequelae may be caused by several CW agents. Cerebral anoxia and brain damage can result from nerve agents, cyanides, and botulinum toxin. Nerve agent poisoning can be followed by prolonged muscular weakness and mental disturbances. Chronic pulmonary fibrosis, bronchiectasis, emphysema, or asthma can be produced by vapor and aerosol attack with vesicating and choking agents. The destruction of the ocular surface by vesicants can lead to permanent blindness from corneal scarring, dry eyes, and chronic irritation. Plastic surgery may be necessary to ameliorate the cicatricial complications of skin damage. Vesicant lung damage may also be followed by an increased risk of lung cancer. Psychiatric and emotional consequences of chemical attack may be severe. The long-term consequences of poisoning with these highly toxic agents are often poorly appreciated [30]; many individuals are, in addition, left with chronic ill-health with reduced exercise tolerance, recurrent infections, hepatic, renal, neurologic, psychiatric, and hematotoxic conditions, and an ill-understood premature aging.

MEDICAL FORENSIC SAMPLES

The first 30 samples from the most contaminated or exposed individuals should rapidly be forwarded to the Centers for Disease Control and Prevention in Atlanta. Samples should have unique but no personal identifiers. The following specimens are requested: (1) 20 ml+ urine samples in screw capped plastic containers; (2) blood serum in two 10 ml containers without anticoagulant (US color-code red top); (3) whole blood in one 5 or 7ml Na oxalate/NaF anticoagulated tube (US color-code grey top) or one 5 or 7ml heparinized tube (US color-code green top); and (4) an empty tube to check as a blank. Chain of evidence documentation must be maintained. Specimens should be shipped refrigerated using Acool-packs and not on dry ice [31]. It is recommended that the state laboratories leave investigation of chemical CW releases to federal laboratories. Environmental sampling is conducted by the EPA and FBI.

SYNDROMIC MEDICAL MANAGEMENT

In view of the potential multiplicity of agents that could be involved in a terrorist attack or accidental chemical release, the specific agent may not be known during the initial phases of patient management. The forensic identification of agents will not be available to aid medical decision-making. The emergency management of chemical injuries may depend upon syndromic identification and the general application of supportive therapies and use of specific therapeutics as a matter of judgement. Table 18.3 illustrates this approach.

LOGISTICS OF THE HEALTH SERVICES RESPONSE TO A CIVILIAN CHEMICAL ATTACK

In the event of most conceivable CW attacks on the homeland, the local and regional capabilities will be decisive in determining the outcome. It is unlikely that a chemical attack could be mounted in the US by a non-statal terrorist group that would lead to more than a few hundred casualties, and might be anticipated to be a much lesser event. Indoor CW attacks in particular need to be incorporated into planning.

Table 18.3 Emergency medical conditions and therapeutic needs associated with chemical exposures.

Syndrome and Causative Agents	Medical Therapeutic Needs
<i>Burns and Trauma</i>	
Corrosives, vesicants, explosives, oxidants, incendiaries, radiologicals	Intravenous fluids and supplies Analgesics Pulmonary care Bandages, splints, and skin care
<i>Respiratory Failure</i>	
Corrosives, CW, explosives, oxidants, incendiaries, asphyxiants, irritants, pharmaceuticals, metals	Pulmonary care Ventilators and supplies Antidotes - if available Tranquillizers
<i>Cardiovascular Shock</i>	
CW, pesticides, asphyxiants, Pharmaceuticals	Intravenous fluids and supplies Cardiovascular care Antidotes - if available
<i>Neurological Toxicity</i>	
CW, pesticides, radiologicals Pharmaceuticals	Antidotes - if available

Source: CDC The Public Health Response to Biological and Chemical Terrorism. Interim Planning Guidance for State Public Health Officials, 2001 [27].

An incremental modular system has to be created that provides surge capacities of several magnitudes for the management of contaminated casualties. Considerable creative planning is being undertaken in the name of homeland defense to provide a system for biological, nuclear, radiological, and chemical terrorist attack on US civilians with 'weapons of mass destruction.' Chemical terrorism is unlikely however to create a threat of this magnitude. Local HAZMAT search and rescue capabilities are well developed in many parts of the US, and there is therefore cumulative experience in the management of accidental chemical releases. Unlike other types of asymmetric terrorism, considerable chemical response infrastructure and professional knowledge is already in existence. Preparedness becomes essentially a matter of degree.

Surge capacities are enhanced by collaborative protocols between local and regional health care organizations and by utilizing support from the state public health system. Federal agencies can provide emergency logistic support through the National Response Plan (Chapter 25), under the crisis management of the FBI and the consequence management of FEMA. Much of the federal effort in bolstering terrorism defense has been in the provision of training programs, and in the development of state and local infrastructure (see Chapter 26) [31-32].

One lesson to be imbedded in local law enforcement is that the requirements for crime scene investigation must take second place to the rescue and resuscitation of persons exposed to these highly toxic chemicals. Normal criminal procedures and perhaps civil rights may require modification in high-level chemical incidents.

With the first appreciation of a potential chemical event involving numerous casualties, local and regional emergency planning agreements will put all emergency hospitals on alert that are within access by road or medivac helicopter. Regional consortial relationships between health centers will be activated to source needed materiel. Patients will be received at local hospitals from the on-site triage center, after preliminary resuscitation and attempted medical stabilization, and often after extensive decontamination. Disaster plans and their chemical emergency annexes will be activated at each health care facility.

The Crisis Management Team (CMT) at each hospital will be activated to function as the institutional command and control center. This is nowadays likely to be accommodated in a formal well-equipped communications facility ideally located away from major operational aspects of the response site. The average size of a CMT is between 5 and 10 with each member responsible for a particular aspect of the operation, such as command, logistics, operations, legal, information, public relations, safety and security, and finance [34]. Only departmental heads will report to the CMT. The hospital responses will be coordinated with the On-site Incident Command Center.

Bed and intensive care availabilities are collated as the magnitude of the emergency is assessed. The immediate establishment of tight hospital security is a critical element if hospital and staff contamination is to be prevented. Early decisions to transfer in-patients to other facilities may be necessary. The hospital chief

pharmacist must be informed of developments to optimize his/her ability to mobilize supplies of the requisite pharmaceuticals and supplies. With some CW agents, there may be considerable surge-demand for emergency respiratory ventilation and intensive care facilities. Consideration may be given to seeking additional ventilatory equipment and supplies through the National Pharmaceutical Stockpile (NPS) which will be delivered within 12 hours from their approval.

The hospital decontamination facilities will need to be greatly enhanced and the engineering and maintenance staff may be required to erect temporary structures and facilities. Triage and patient observation areas may also need to be provided. Contaminated, intermediate, and clean areas must be established with obvious boundary markers, and the sanctity of each area enforced by security officers in PPD. Efficient medical record keeping is required, modified by the demands of the situation. A cadre of officials should be delegated to maintain chain of security and documentation of anything that could be considered evidentiary, including the possessions of victims and of medical specimens. Additional mortuary facilities may be required, as well as provision for the decontamination of the deceased. From the outset, information provided to the public and press must be timely, professional, comprehensive, and honest.

The regional Metropolitan Medical Response System (MMRS) and the National Disaster Medical System (NDMS) will be activated by the FEMA National Emergency Coordinating Center (NECC) and by the Department of Health and Human Services Emergency Operations Center (DHHS EOC) so as to mobilize regional assets into the emergency response. A Disaster Medical Assistance Team (DMAT) may be available from the MMRS for immediate engagement at the incident site. A specialist Chemical DMAT may also be available. The Veterans Administration may be able to deploy an Emergency Medical Response Team (EMRT). The proximity of these assets to the incident site will determine whether they might play a role in the emergency phase of the response or contribute to the mitigation phase. Local National Guard units could be activated by the state governor under title 32 to help with the many logistic tasks that occur during a substantial chemical emergency. As the first responders, the local and state emergency response leadership will set up an emergency operating center to coordinate the HAZMAT search and rescue phase. The FBI will be involved as soon as possible and will ultimately assume the leadership role of the crisis management.

The resources and assets mobilized will depend upon the magnitude and nature of the chemical release, in consultation with the state and FEMA authorities. Small events can be managed in a manner similar to a conventional HAZMAT event, with the addition of considerable FBI and law enforcement activity. Mass casualties will necessitate a full mobilization of the Federal Response Plan following a declaration of emergency by the US President under Emergency Support Function (ESF) #8, in which the DHHS is the lead agency. These procedures are discussed in detail in Chapter 26.

There are a number of federal specialist chemical response teams that also might play a role in a CW civilian attack [35]. It is only in the case of predeploy-

ment at an event such as the Olympic Games or national election that federal assets might influence the outcome of rescue operations. Military chemical response establishments are operated by the Marine Corps, Army (Technical Escort Unit: TEU), Air Force (BEEF Unit), Army Reserve Chemical Companies, National Guard Chemical Units, and Coast Guard Units. Military assets are obtained by state request under the National Response Plan to the Department of Defense Joint Task Force-Civil Support Unit (JTF-CS). The EPA possesses emergency contamination clean-up teams that may be useful if there is a markedly contaminated environment.

A major CW attack will generate considerable logistical and personnel problems if operations are to continue at high intensity throughout the medical emergency. But there will be other requirements, such as to maintain essential services and to ameliorate the many consequences of chemical warfare within a community. The greatest need will often be for trained personnel with all kinds of skills and the flexibility to take on almost anything. The contaminated area will have to be cordoned off and guarded until the environmental decontamination is completed. There may be considerable need for temporary housing and support structures should a residential area be involved.

The general public must be involved before, during, and following any CW attack. There are considerable misconceptions about the nature of chemicals and the about the alleged vulnerability to foreign terrorist attack in the local high street. If people are educated, as a policy matter, about how the public should respond to accidental releases of hazardous materials from, say, a neighborhood chemical plant, and are then taken as full partners into the confidence of local and national leadership should convincing CW terrorism threats arise, the resolution of the American people will be a crucial strength if the civilian population is ever targeted.

REFERENCES

1. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. Geneva, Switzerland: Organization for the Prohibition of Chemical Weapons, 1994. Internet: <http://www.opcw.org/cwc/cwc-eng.pdf> Accessed April 6, 2002.
2. National Disaster Education Coalition. Chemical Emergencies. Internet: <http://www.disastercenter.com/guide/chemical.html> Accessed April 6, 2002.
3. Binder S. Deaths, injuries and evacuations from acute hazardous material releases. *Am J Public Health* 1989;79:1042-1044.
4. US Department of Health and Human Services. Managing Hazardous Materials Incidents (MHMI), vol 1, 2, and 3. Atlanta, GA: Agency for Toxic Substances and Disease Registry, 2001. Internet: <http://www.atsdr.cdc.gov/mhmi.html> Accessed April 6, 2002.

5. Chemical Casualty Care Division, US Army Medical Research Institute of Chemical defense. Medical Management of Chemical Casualties Handbook, 3rd edit. Aberdeen Proving Ground, MD: USAMRICD, 2000. Internet: http://ccc.apgea.army.mil/reference_materials/handbooks/Red-Handbook/001TitlePage.htm, Accessed April 6, 2002.
6. Committee on Environmental Health and Committee on Infectious Diseases, American Academy of Pediatrics. Chemical and biological terrorism and its impact on children. *Pediatrics* 2000;105:662-670. Internet: <http://www.aap.org/policy/re9959.html> Accessed April 6, 2002.
7. WHO Group of Consultants. Health Aspects of Biological and Chemical Weapons: WHO Guidance, edit 2. Geneva, Switzerland: World Health Organization, 2002. Internet: http://www.who.int/emc/book_2nd_edition.htm, Accessed April 6, 2002.
8. Falkenrath RA, Newman RD, Thayer BA. America's Achilles Heel. Nuclear, Biological, and Chemical Terrorism and Covert Attack. Cambridge, MA: MIT Press, 1998.
9. Taylor ER. Lethal Mists: an Introduction to the Natural and Military Sciences of Chemical, Biological Warfare and Terrorism. Commack, NY: Nova Science, 1999.
10. Kaplan DE. Aum Shinrikyo. In: Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons. Tucker JB, ed. Cambridge, MA: Belfer Center for Scientific and International Affairs, Harvard University, 2000, pp 207-226.
11. US Department of Justice. Emergency Response to Terrorism Self-Study. Washington DC: Federal Emergency Management Administration, 2002. Internet: <http://www.usfa.fema.gov/pdf/ertss.pdf> Accessed April 6, 2002.
12. Interagency Intelligence Committee on Terrorism. Chemical/ Biological/ Radiological Incident Handbook. Washington DC: Central Intelligence Agency, 1998. Internet: http://www.cia.gov/cia/publications/cbr_handbook/cbrbook.htm Accessed April 6, 2002.
13. Erickson PA. Emergency Response Planning for Corporate and Municipal Managers. San Diego: Academic Press, 1999.
14. Macintyre AG, Christopher GW, Eitzen E, Gum R, Weir S, DeAtley C, Tonat K, Barbera JA. Weapons of mass destruction events with contaminated casualties. Effective planning for health care facilities. *JAMA* 2000;283:242-249. Internet: <http://jama.ama-assn.org/issues/v283n2/ffull/jsc90100.html> Accessed April 6, 2002.
15. Rivkind A, Barach P, Israeli A, Berdugo M, Richter E. Emergency preparedness and response in Israel during the Gulf war. *Ann Emerg Med* 1997;30:513-521.
16. US Department of Transportation/ Transport Canada/ Secretariat of Communications and Transportation of Mexico. North America Emergency Response Guidebook, 2001. Internet: <http://hazmat.dot.gov/guidebook.htm> Accessed May 8, 2002

17. Chemical Manufacturers Association. Chemtrec, Internet: <http://www.cwc-chemical.com/chemtrec.htm> Accessed: May 8, 2002.
18. Burgess J, Kirk M, Borron S, Cisek J. Emergency department hazardous materials protocol for contaminated patients. *Ann Emerg Med* 1999; 34:205-212.
19. Staten CL. Emergency Response to Chemical/ Biological Terrorist Incidents. Chicago: Emergency Response and Research Institute, 1997. Internet: <http://www.emergency.com/cbwlesn1.htm> Accessed April 6, 2002.
20. Organization for the Prohibition of Chemical Weapons. Chemical warfare agents: an overview of chemicals defined as chemical weapons. Geneva: Switzerland: OPCW, 2002. Internet: <http://www.opcw.org/resp/html/cwagents.html> Viewed April 6, 2002.
21. Sullivan J, Krieger G. Hazardous Materials Technology. Baltimore: Williams & Wilkins, 1992.
22. Keim M, Kaufman AF. Principles for emergency response bioterrorism. *Ann Emerg Med* 1999; 34:183-190.
23. Waeckerle JF. Domestic preparedness for events involving weapons of mass destruction. *JAMA* 2000;283:252-254. Internet: <http://jama.ama-assn.org/issues/v283n2/ffull/jed90095.html> Accessed April 6, 2002.
24. Swedish Defence Research Agency. A FOA Briefing Book on Chemical Weapons: Threats, Effects, and Protection. Stockholm, Sweden: FOA, 1995.
25. Marrs TC, Maynard RL, Sidell FR. Chemical Warfare Agents: Toxicology and Treatment. Chichester, UK: John Wiley, 1996.
26. Noeller TP. Biological and chemical terrorism: recognition and management. *Cleveland Clin J Med* 2001;68:1001-1016. Internet: <http://www.ccm.org/pdffiles/BioTerror.pdf> Accessed April 6, 2002.
27. Franz DR. Understanding the Threat. Defense Against Toxin Weapons, chapter 1. Iowa City: Virtual Naval Hospital, University of Iowa, 2002. Internet: <http://www.vnh.org/DATW/chap1.html> Accessed April 6, 2002.
28. North Atlantic Treaty Organization. Nato Handbook on the Medical Aspects of NBC Defensive Operations, Part III Chemical, AmedP-6(B). Washington DC: Departments of the Army, the Navy, and the Air Force, 1996. Internet: <http://www.fas.org/nuke/guide/usa/doctrine/dod/fm8-9/3toc.htm> Accessed April 6, 2002.
29. Sidwell FR, Takafuji ET, Franz DR, eds. Medical Aspects of Chemical and Biological Warfare. In: Textbook of Military Medicine, Zajtcuk R, Bellamy, eds, Series Part 1, Warfare, Weaponry, and the Casualty. Washington DC: TMM Publications, Borden Institute, 1997. Internet: <http://chemdef.apgea.army.mil/textbook/contents.asp> Accessed April 6, 2002.

30. Stockholm International Peace Research Institute. Delayed Toxic Effects of Chemical Warfare Agents. Stockholm: Almqvist & Wiksell, 1975. Internet: <http://projects.sipri.se/cbw/research/cw-delayed.pdf> Accessed: April 6, 2002.
31. Centers for Disease Control and Prevention. The Public Health Response to Biological and Chemical Terrorism. Interim Planning Guidance for State Public Health Officials. Washington DC: US Department of Health and Human Services, 2001. Internet: <http://www.bt.cdc.gov/Documents/Planning/PlanningGuidance.PDF> Accessed April 6, 2002.
32. General Accounting Office. Chemical and Biological Defense Units Better Equipped, but Training and Readiness Reporting Problems Remain, GAO-01-27. Washington DC: GAO, 2001. Internet <http://www.gao.gov/new.items/d0127.pdf> Accessed April 6, 2002.
33. Centers for Disease Control and Prevention Strategic Planning Group. Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response. MMWR Morb Mortal Wkly Rep 2000;49(RR-4):1-14. Internet: <http://www.bt.cdc.gov/Documents/BTStratPlan.pdf> Accessed April 6, 2002.
34. Knapp WM, Knapp LA. Biological and Chemical Terrorism and the Medical Preparedness Paradigm. A Protective Research Group Perspective. Internet: <http://www.proresearchgroup.com/articles/BC%20Report.pdf> Accessed April 6, 2002.
35. Smithson AE, Levy L-A. Ataxia: the Clinical and Biological Terrorist Threat and US Response, Stimson Center Report No. 15. Washington DC: HL Stimson Center, 2002. Internet: <http://www.stimson.org/pubs.cfm?ID=12> Accessed April 6, 2002.

19

Chemical Weapon Delivery, Sensors and Detection Systems

Mark A. Prelas and Tushar K. Ghosh

University of Missouri, Columbia, Missouri

INTRODUCTION

Methods of delivery for chemical weapons have been under development since World War I. The science and technology of dispersion and dissipation of chemical agents range from the sophistication of weapons of war to the simple for the purpose of terrorism. This chapter discusses how chemical agents are dispersed and dissipated. In addition, this chapter covers the topic of trace chemical sensors. Such sensors are available and can detect chemical vapors in the sub-parts-per-billion range or in the sub-picogram range. The capability of trace chemical sensors provides a valuable counter terrorism tool.

DELIVERY SYSTEMS

As discussed in chapter 6, the key to effective use of either biological agents or chemical agents is the dispersion and dissipation of the agent. The routes for exposure to chemical agents are:

- Inhalation from vapor
- Skin contact from vapor or liquid
- Ingestion from liquid

During World War I, chemicals such as chlorine, mustard gas and phosgene were released in vapor form. More sophisticated weaponization techniques deliver

the agent in a fine mist or spray. Many countries have weaponized chemical agents. For example, the United States began developing chemical munitions in 1950. A wide variety of projectiles, mines, bombs and sprayers were developed.

Projectiles were developed for direct use of GB or VX. The agent was placed in a shell along with a fuse and a bursting charge. A simplified shell is shown in Figure 19.1.

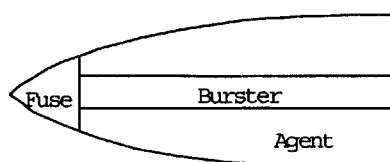


Figure 19.1 Simplified diagram of a shell.

Examples of shells include a 4.2 inch mortar shell (e.g., M2A1), 105 mm, 155 mm and 203 mm Howitzer projectiles (e.g., M360 GB, M121A1 GB or VX and M426 GB or VX). Binary shells were also developed in which the mixture of two relatively benign chemicals formed GB or VX. These binary shells include the 155 mm M687 GB-2 projectile and the 203 mm XM736 VX-2 projectile.

A number of munitions were developed for air delivery including bombs and spray tanks. The bombs include the M134 GB cluster, the 750 pound MC1, the 500 pound MK116, and the BLU 80/B binary VX.

Spray tanks were also developed for air delivery including the Aero 14B and a TMU 28B cruise missile with spray tank. The Aero 14B was very much like a spray tank used in crop dusters.

Chemical agents were also used in missiles. Examples of these include the Little John (M206), the Honest John (M79), the improved Honest John (M190) and the Sergeant (M212). A warhead is more complex than a shell in that it is filled with submunitions or bomblets such as the M139. The submunitions have a similar design as a shell in that there is a fuse, a burster and an agent. The submunitions are designed to take disperse flight paths so as to cover the maximum area when they burst. Figure 19.2 shows an Honest John missile. An illustration of the warhead is shown in Figure 19.3.

Small-Scale Delivery

Munitions are a very effective means of delivering a lethal dose of agent over a large area because they were designed for military use. However, munitions are not the only means of delivery. Chemical agents can be delivered on a small-



Figure 19.2 An Honest John Missile with launcher.

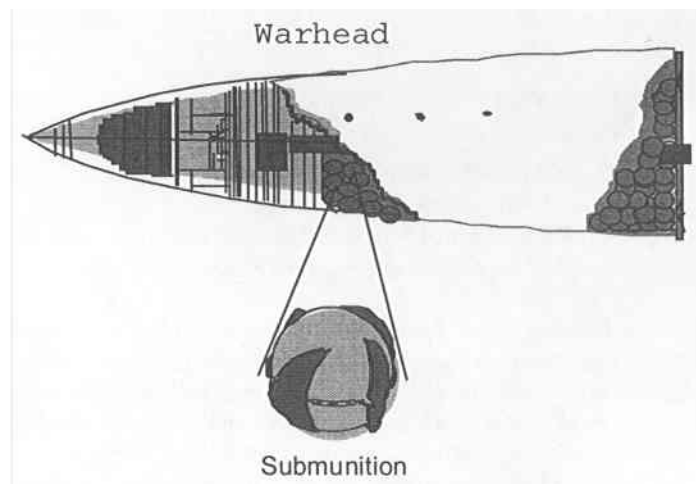


Figure 19.3 Illustration of a warhead filled with submunitions or bomblets.

scale by potential terrorists. On March 20, 1995 the doomsday cult Aum Shinrikyo attacked the subway in Tokyo with sarin (1,2). A man in a surgical mask sat down

in the eighth car of the B711T train on Tokyo's Hibiya line. He pierced a plastic bag containing sarin and left it on the floor and a liquid puddle formed. Soon afterwards passengers around the puddle took ill. All in all, five such bags were placed in subway cars simultaneously and the attack resulted in 12 deaths and 5000 injuries. Had the sarin been delivered more effectively, there is no telling how high the death total would have been.

In order to effectively deliver the agent, it must be aerosolized. Aerosolization can be achieved in many ways. For example, a simple garden sprayer is very effective in aerosolizing chemicals. Sprayers have been designed for crop dusters so as to allow the maximum coverage of an area with a chemical.

CHEMICAL DETECTION

Detection of chemical agents is important. One of the worst scenarios is to identify an attack with chemical agents by observation: 1) visible cloud drifts towards the observer, 2) people fall ill and show symptoms of poisoning, and 3) observations are made of dead animals. Trace chemical sensors are a preferable means of detection. The wide deployment of trace chemical sensors is still years away, but great strides in trace chemical detection technology are being made. When these technologies come to fruition, it may be feasible to set up early warning networks in strategic areas or to identify an agent or its precursors prior to release in order to foil potential attacks.

Detection of chemical agents is needed to address the following basic questions:

- Is there an agent present?
- What is the agent?
- Is a mask required?
- Is body protection necessary?
- Should normal behavior should be modified in any special way?
- Will the emergency response equipment require decontamination?

Detection is needed for different purposes. Ideally, a chemical detector should serve multiple purposes. One purpose is for an alarm system. Such a system would continuously monitor the environment with a sensor array for the presence of chemical agents. Such sensor arrays could serve as an advanced warning system for attack with chemical agents provided that it is easy to use, requires minimal personnel training and is capable of triggering an alarm if a defined minimal level of chemical agent is detected. It is also important that the sensor indicate when the contaminated area is safe since it is very difficult to work in protective clothing and it is desirable to minimize personnel time in the clothing. The sensor should be useful in the verification and identification of agents. Deci-

sions on how to respond to a chemical attack require that you know the type of agent and its concentration. Different types of detection require different types of equipment and methods. (For example, is the gas concentration in the air at a dangerous level, is the soil or equipment contaminated with liquid agent, is it dangerous to handle?) Sensors for mapping of the ground contamination would be valuable in order to indicate the bounds of the contamination. Unfortunately, the state of the art technology does not meet all of the requirements of an ideal chemical detector. Technologies which exist or are being developed show great promise in achieving the goals of an ideal detections system. Current systems include detection (enzyme) tickets and detection tubes which can be used for nerve agents and mustard agent under field conditions. A manual suction pump is used to draw air through the detection tube or against the ticket. There is a development process to determine the agent.

Detection (enzyme) tickets consist of two parts, one with enzyme-impregnated paper and the other with substrate-impregnated paper. When the package is broken and the enzyme paper wetted, the substrate part is exposed to the agent by means of a pump. The two parts are put together. If the enzyme part of the ticket has turned a light blue color, the nerve agent is present in the air. The detection limit is about 0.02-0.05 mg/m³. The active enzyme, some form of cholinesterase is used, which changes to a blue color in the presence of nerve agents:

2,6-dichloroindophenylacetate (red) + cholinesterase produces 2,6-dichloroindophenol (blue)

The detection tube for mustard agent is a glass tube containing silica gel impregnated with a substrate (DB-3). Sample air is sucked through the tube using a special pump. Using heat, a reaction occurs between the mustard agent and substrate. A developer is then added. If the silica gel in the tube turns blue, then the sample contains mustard agent.

Substrate Reaction with Mustard:

$\text{Cl}(\text{CH}_2)_2\text{S}(\text{CH}_2)_2\text{Cl}$ (mustard agent) + pyridine- CH_2 -p-phenylidene- NO_2 (4-(4-nitrobenzyl)pyridine, colorless)

reacts at 110 °C in the presence of NaOH to provide

$\text{Cl}(\text{CH}_2)_2\text{S}(\text{CH}_2)_2\text{N}=\text{CH}$ -pyridine- NO_2 (1-[1-[2-(2-chloroethylthio)ethyl]-1,4-dihydro-4-pyridylidene]methyl]-4-nitrobenzene, blue)

In mapping of ground contamination it is necessary to map which parts of an area are contaminated with CW agents in liquid form. In this case, detection paper has been the method of choice. Detection paper (e.g., M9 and M8 chemical agent detector papers) is based on certain dyes being soluble in CW agents. Two dyes and one pH indicator are used, which are mixed with cellulose fibers in a paper

without coloring. The chemical agent is absorbed by the paper, and it dissolves one of the pigments. Mustard agent dissolves a red dye and nerve agent a yellow. In addition, VX causes the indicator to turn to blue which, together with the yellow, will become green/green-black. There is a disadvantage in that many other substances can also dissolve the pigments. Consequently, detection paper should not be located in places where drops of solvent, fat, oil or fuel can fall on them. Drops of water give no reaction. A droplet of 0.5 mm diameter creates a spot sized about 3 mm on the paper. This size droplet corresponds to a ground contamination of about 0.5 g/m². The detection limit in favorable cases is 0.005 g/m².

Trends in detectors are very promising and are fully discussed the next section. Some of the important developments are:

- Ion mobility detector IMS (Ion Mobility Spectroscopy), the Chemical Agent Monitor (CAM), (e.g., the Finnish M86 and the more recent M90).
- Flame photometry FPD (Flame Photometric Detector—uses a hydrogen flame burns the sample of air, the color of the flame is examined by a photometer. The presence of phosphorus and sulfur can be seen).
- French monitor AP2C and Israeli combined detector and monitor CHASE.
- Enzymes are being developed in the United Kingdom, Netherlands and former Soviet Union.
- Optical methods (IR) being developed in the US and France.
- Biologically active molecules as sensors—same mechanisms that influence the human body when exposed to poisoning. A simple type of biosensor is the enzyme ticket.

TECHNIQUES FOR CHEMICAL VAPOR DETECTION

It is important to note that technology is available for the detection of trace chemicals. A number of technologies are being used in the field, are well along in development or potentially could be developed. These methods can be used solely for explosives or for a variety of chemical agents. Here a number of methods for detecting chemical vapors are discussed along with their potential uses.

These methods are divisible into several categories each with strengths and weaknesses. A discussion of each category of trace chemical detector is described. One should pay attention to the detection time, sensitivity, portability, cost, data gathering and ability to differentiate different chemical agents. A definition of each of these categories is given below:

- The detection time is defined as the time that it takes the detector to respond to the presence of vapors from a chemical agent and/or a high explosive.
- The sensitivity of the detector is defined as the minimum amount of chemical vapor and/or high explosive material that the detector will respond to. This may be defined in parts per billion in air or in nanograms. Some sensors respond in real time to the vapor being flowed through its active region. In this case parts per billion in air is a direct correlation of the sensor's ability to distinguish vapors in air. Some sensors can accumulate molecules on a detector surface over a long sampling time. In this case the use of nanograms provides the most accurate information on sensitivity.
- The portability of the detector system is comprised of the size, volume and mass of the system.
- The cost of the detector system is the combination of purchase price, operational costs, and maintenance costs of the system.
- Data gathering is the ability to detect multiple chemical agents with a single sensor system.
- Differentiation is defined as the ability of the detector to differentiate between chemical agents
- Field_deployed indicates if the unit has been deployed in the field and field-tested.
- Suitability indicates the technology's potential for use in the field as a general chemical sensor.

Canine

Canine explosive detection is a unique category. Trained dogs have been used in the field successfully for a very long time. Dogs are able to detect small amounts of drugs or of explosive material and are able to distinguish types of explosive if properly trained. No chemical sensor has been able to match a "dog's nose" for sensitivity. For example, dogs are a key component for the South African Mechem Explosive and Drug Detection System (MEDDS) [3,4]. In the MEDDS, a chemical concentrator system is used to collect vapors and this collected material is passed by the dog's nose. Dogs should be able to detect other types of chemical agents or their precursors if properly trained.

There are problems however; dogs are only able to work for about two hours at a time and not always able to perform at peak condition. In addition, dogs have a 95% success rate.

Analysis of Canine

Dogs have been field deployed. They do not appear to be a practical alternative for a portable field unit. The portability of the canine is of concern. A working

period of 2 hours per canine requires that a large pool of canines must be available for continuous monitoring. Additionally, each animal is unique; thus the operation and result from animal to animal would be slightly different. Finally, a success rate of 95% is good.

- Detection Time: seconds
- Sensitivity: Excellent (better than man-made chemical detectors)
- Portability: Poor
- Cost: moderate
- Data Gathering: low
- Differentiation: potentially excellent depending on training
- Field Deployed: yes

DIFFUSION METHODS

Gas Chromatograph (GC)

A Gas Chromatograph (GC) uses a column of material(s) in which gases of different mass diffuse at different rates, which is the mechanism for differentiation. Lighter gases will have a higher rate of diffusion than a heavy gas. Thus the time it takes gas molecules to move through the column is directly related to the mass of the gas molecule. The time it takes from the sample introduction into the column to its exit from the column is the parameter used to distinguish between gas molecules. Gas chromatographs are typically combined with other sensor technology.

Analysis of GC

As a stand-alone unit, a GC has been field deployed. It has very little utility in field use. However, combined with other sensors, as will be described, it is a very useful technology.

- Detection Time: 10-15 seconds
- Sensitivity: Good to Excellent (depending on sensor technology)
- Portability: Excellent
- Cost: Low
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

IONIZATION-BASED SENSORS

Ionization-based sensors use either an electrical field or a source of electrons to ionize the gas sample. A number of ionization-based sensors are described.

Electron Capture Detector (ECD)

A tritium or Ni^{63} radioisotope beta emitter is placed opposite a positively biased electron collector (as shown in Figure 19.4). Helium or argon gas flows between the radioisotope and collector plate. Interactions between helium and argon with energetic electrons are well understood. The electron current collected by the plate comes into equilibrium with its environment. If a vapor of a molecule that can form a negative ion by electron capture is introduced into the gas flow, the electron current from the collector plate is reduced. This reduction in current is related to the molecule. The electron capture rate is proportional to the density of the molecule.

The device is primarily used for explosives but is not able to distinguish between explosives. Also, any molecule that has a high electron capture cross section such as oxygen, carbon halides, carbon dioxide, carbon monoxide, halides, etc. will cause a false trigger.

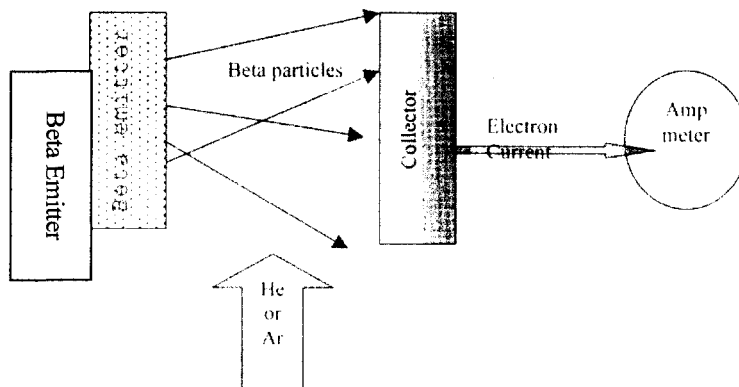


Figure 19.4 Diagram of Electron-Capture Detector (ECD).

Analysis of ECD

The stand alone ECD has been field deployed. It is not very useful for field use.

- Detection Time: sub second
- Sensitivity: Good (1 part per billion)
- Portability: Excellent
- Cost: Low
- Data Gathering: Low
- Differentiation: None
- Field Deployed: Yes

If the ECD is placed on top of a GC, then the combined instrument does have the capability of differentiating explosive materials. (Figure 19.5). In this case, the collector current is measured as function of time. The time is matched to the diffusion rate of the molecule in the GC column (Figure 19.6).



Figure 19.5 A GC combined with ECD.

Combined GC and ECD units are sold commercially like the Exdetex02 made by Jasmin Simtec Ltd.

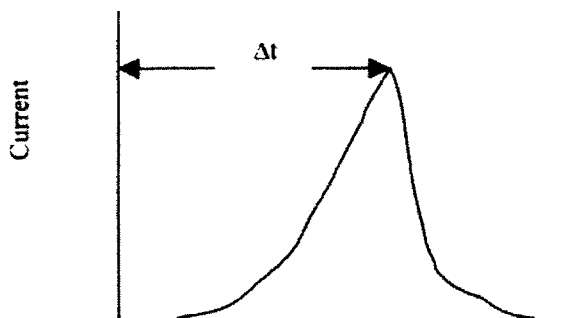


Figure 19.6 The current is measured as a function of time. The time delay Δt , is related to the diffusion time of the molecule in the GC.

Analysis of ECD Combined with GC (ECD/GC)

The ECD combined with a GC has been field deployed. It is able to differentiate explosives in about 18 seconds with a sensitivity of 1 part per billion. The sensitivity may be adequate for TNT depending on the sealing method that is used, but not for plastic explosives (e.g., RDX). A great deal of data can be gathered with the combined ECD and GC.

- Detection Time: about 18 seconds
- Sensitivity: Good (1 part per billion)
- Portability: Excellent
- Cost: Low
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

Ion Mobility Spectrometry (IMS)

The principle of Ion Mobility Spectrometry (IMS) is that in an electric field the drift velocity of an ion is mass dependent. The drift velocity, \mathbf{u} , of an ion in an electric field is proportional to the electric field with the ion mobility being the proportionality constant.

$$\mathbf{u} = \mu \mathbf{E} \quad \text{Eq. 1}$$

where, \mathbf{u} is the drift velocity of the ion, μ is the ion mobility and \mathbf{E} is the electric field vector. (A bold symbol represents a vector quantity.)

Based on the length of time that it takes an ion to travel a fixed distance, the ion mass can be determined. The IMS is constructed to first create ions with an ionization source. The ions enter a region of known electric field through a grid electrode and then drift towards an ion collector (See Figure 19.7).

A number of commercial units based on IMS are available. For example, the Itemiser E and Exfinder 152 are both manufactured by AI Cambridge Ltd. Another unit, which is of Russian manufacture, is the MO2 portable high-sensitivity explosives vapor detector produced by the Institute of Applied Physics.

Analysis of IMS

IMS technology has been field deployed. It is a viable technology for use in the field. It is sensitive, can differentiate, portable and low cost. IMS can generate a large amount of data on multiple chemicals. IMS is very adaptable.

- Detection Time: about 5-8 seconds
- Sensitivity: Good (sub-nanogram)
- Portability: Excellent
- Cost: Low
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

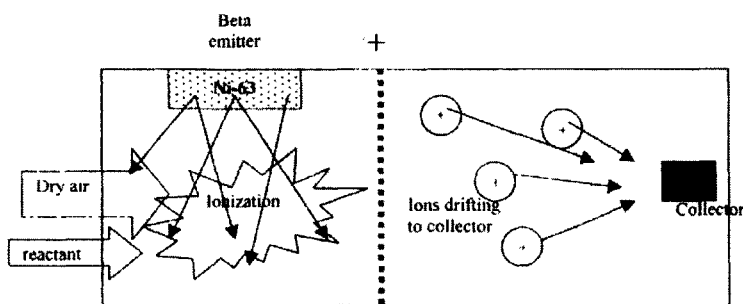


Figure 19.7 Diagram of the Ion Mobility Spectrometer (IMS).

Field Ion Spectrometry (FIS)

FIS is similar to IMS. In FIS a transverse electric field (meaning perpendicular to the path between the grid and the collector) with both an AC (alternating current) and DC (direct current) component is added (see Figure 19.8). Based upon the ion mass, the rate at which the ion moves transverse to the collection path is dependent upon the mass of the ion. When the DC component of

is dependent upon the mass of the ion. When the DC component of the transverse field is varied, a spectrum of ion current is collected. The data collected will be a curve in which DC voltage is plotted on the x-axis and the ion current on the y-axis. The FIS data is manipulated mathematically and is converted to a plot of mass versus DC voltage. In the IMS, time is plotted on the x-axis and ion current on the y-axis. The IMS data is manipulated mathematically and is converted to a plot of mass versus time. The advantage of the FIS is that the sample can be continuously introduced into the spectrometer while the IMS requires the grid field and sample introduction to be timed with a pulsing mechanism.

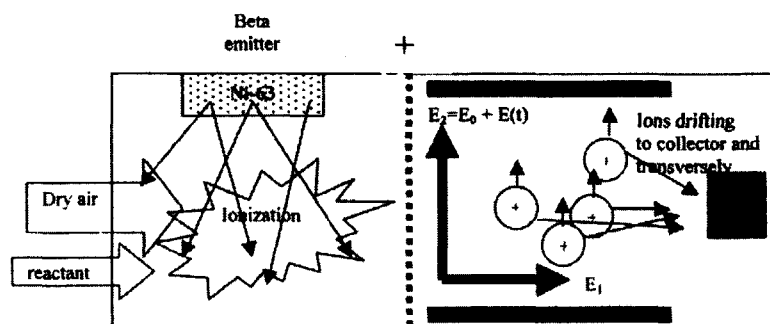


Figure 19.8 Diagram of FIS. The collector path electric field is E_1 while the transverse electric field is E_2 , which is made up of a DC component E_0 and a time-dependent component $E(t)$. The field E_0 is varied to obtain data.

Analysis of FIS

FIS has been field deployed. It is a viable technology for use in the field. It is sensitive, and can differentiate, is portable and low cost. FIS can be used for multiple chemical agents and thus can provide a large amount of data.

- Detection Time: about 2 seconds
- Sensitivity: Excellent (picogram)
- Portability: Excellent (size about 0.8 ft³)
- Cost: Low
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

Mass Spectroscopy (MS)

Mass spectroscopy in general uses an ionization region followed by some combination of electromagnetic fields to separate ion mass. Mass spectroscopy is very sensitive, reliable and viable for use in the field. Many system configurations are possible beyond those described here. A major consideration for a specific mass spectroscopy configuration is its level of development. Some mass spectroscopy configurations are well developed but are not suitable for field use. For example a number of systems such as the time of flight mass spectrometer are not portable.

Tandem Mass Spectrometer (TMS)

Oak Ridge National Laboratory is developing a Tandem Mass Spectrometer (TMS). The TMS has a high efficiency ion source. The system is in the testing phase but is not field deployable yet. This system is mentioned because of its high sensitivity that may be of interest for future considerations.

Analysis of TMS

At this point TMS has **not** been field deployed. It is however a promising technology.

- Detection Time: several minutes
- Sensitivity: Excellent (sub-picogram)
- Portability: Unknown
- Cost: Unknown
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: No

METHODS THAT DEPEND ON UV-IR PHOTONS

A number of chemical sensing methods depend on the absorption, scatter or emission of Ultra Violet (UV) and Infra Red (IR).

Chemiluminescence (ChL)

When a chemical vapor of certain nitrogen-rich explosives is heated, the gas NO is created. Using this principle, it is possible to build a Chemiluminescence sensor. The sensor works by interacting the NO with a stream of ozone (O₃) to form NO₂^{*} (see Figure 19.9). The superscript “*” indicates an excited vibrational state in NO₂. This excited vibrational state in NO₂^{*} emits an IR sensitive photomultiplier (PM) tube. The signal from the PM tube is directly proportional to the NO

concentration. A density of the chemical vapor from the explosive sample can be related to the amount of NO produced by heating.

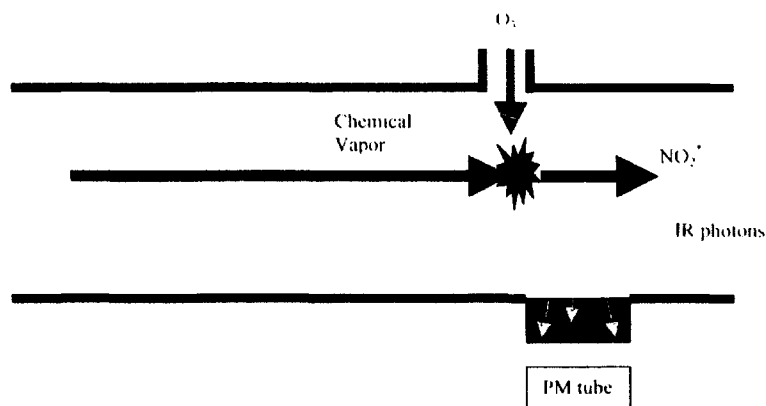


Figure 19.9 A diagram of the chemiluminescence detector.

The chemiluminescence detector is not explosive-specific since most nitrogen-rich explosives will produce NO by this method.

Analysis of Chemiluminescence

As a stand-alone high explosive chemical vapor sensor, it is able to give a positive or negative result. It is not able to distinguish between explosive materials.

- Detection Time: 10 seconds
- Portability: Good
- Cost: Good
- Data Gathering: Low
- Differentiation: None
- Field Deployed: Yes

Combining a Chemiluminescence detector with a GC does provide a system that can differentiate between explosives.

Analysis of Chemiluminescence Combined with GC

A ChL/GC detector has been field deployed for high explosives. A combined Chemiluminescence with a GC is able to distinguish between explosive materials. The sensor is not capable of being used to sense anything other than an explosive because only chemical vapors from nitrogen-rich compounds can form NO. Thus

it has a low data-gathering potential. Chemical vapors from other agents are not detectable.

- Detection Time: 18 seconds
- Sensitivity: Excellent (sub-picogram)
- Portability: Good
- Cost: Moderate
- Data Gathering: Moderate to High
- Differentiation: Excellent
- Field Deployed: Yes

Raman Scattering (RS)

“When a beam of light passes through a solid, liquid or gas a small part of the scattered radiation has the wavelength shifted by a constant amount. The constant change in wavelength or frequency is characteristic of the material which is scattering the light, and corresponds to the frequency of vibration or the frequency of rotation of the molecules of the material. This particular type of scattering is Raman scattering [5].” Even though commercial chemical vapor sensors using Raman scattering are not common, Raman scattering is nonetheless very powerful. The system is relatively simple to construct (see Figure 19.10).

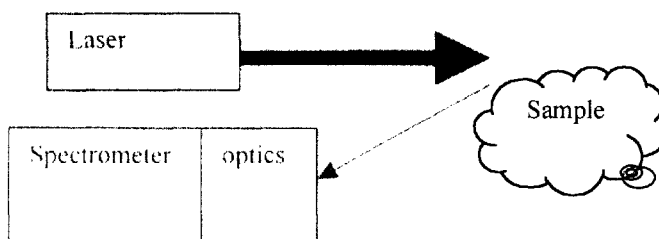


Figure 19.10 Illustration of a Raman scattering system.

Analysis of Raman Scattering

Raman scattering is an effective chemical sensing system that has **not** been field deployed thus far in this application. It can be made portable, sensitive, and can differentiate between chemical vapors. The question is how sensitive it will be with chemical vapors from the scattering from specific agents. For example

graphite scatters 50 times more light than diamond despite the fact that both materials are made of carbon.

- Detection Time: sub-second
- Sensitivity: Unknown (material-dependent)
- Portability: Good
- Cost: Moderate
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: No

Absorption Spectroscopy (AS)

Molecules will absorb light. The exact wavelengths and absorption cross section are dependent upon the molecule's quantum structure. AS is a well known technique. However, specific AS systems for the detection of vapors from chemical agents and explosives are not available. An AS system is relatively simple to construct (Figure 19.11).

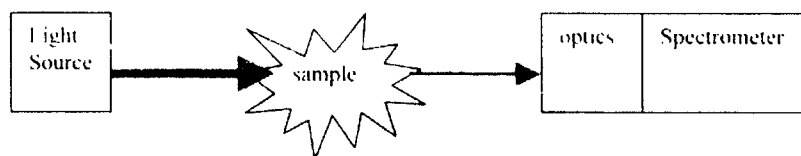


Figure 19.11 A diagram of an absorption spectroscopy system.

Analysis of AS

AS is an effective chemical sensing system that has not been field deployed for this application. It can be made portable, sensitive, and can differentiate between chemical vapors. The question is how sensitive it will be with chemical vapors from specific agents. Various materials behave differently with AS. The sensitivity is dependent upon the absorption cross section at various wavelengths, the availability of optics at the absorption wavelengths, the availability of a spectrometer for the absorption wavelengths and the availability of a sensitive photon detector at the absorption wavelengths.

- Detection Time: sub-second
- Sensitivity: Unknown (material-dependent)
- Portability: Good

- Cost: Unknown (depending on frequency)
- Data Gathering: Low (frequency-specific)
- Differentiation: Excellent
- Field deployed: No

Optical Fiber Sensors (OFS)

Glass fibers with a thin chemically active coating on the sides or ends can respond to the presence of a volatile organic compound [6]. A single frequency or narrow band frequency light source enters the fiber. The chemically active material containing fluorescent dyes immobilized in an organic polymer matrix is used. The volatile organic compound reacts with the thin active coating and the light source by altering the polarity of the dyes. This interaction shifts the fluorescent spectrum (Figure 19.12).

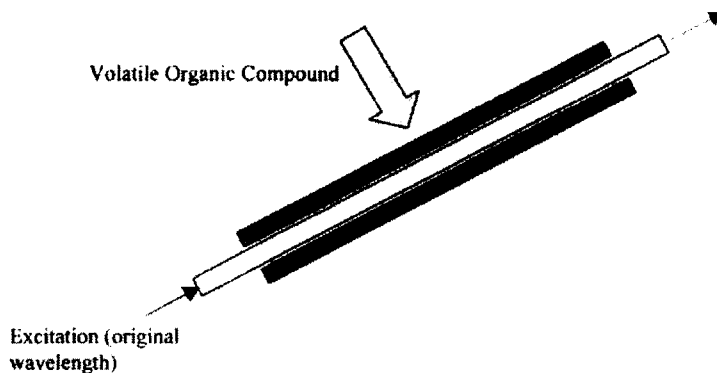


Figure 19.12 Optical-Fiber sensor that employs a glass fiber and a chemically active coating. This coating interacts with an excitation light source by shifting its response frequency.

Analysis of OFS

OFS is an effective chemical sensing system that has not been field deployed for this application. It can be made portable, sensitive, and can differentiate between chemical vapors but is dependent on the active material. The question of sensitivity has yet to be answered.

- Detection Time: sub-second
- Sensitivity: Unknown (material-dependent)
- Portability: Good
- Cost: Unknown (depending on frequency)

- Data Gathering: Low (frequency and active chemical specific)
- Differentiation: Excellent
- Field Deployed: No

Acoustic-to-Optic Tunable Filters (ATOFs)

The ATOFs alter the light filtering properties of a material in response to a change in voltage across the materials light transmission path.

Analysis of ATOFs

ATOFs are in the research phase. Little can be reported at this time about the potential of the approach.

- Detection Time: sub-second
- Sensitivity: Unknown (material-dependent)
- Portability: Good
- Cost: unknown (depending on frequency and material)
- Data Gathering: Low (frequency and material specific)
- Differentiation: Excellent
- Field Deployed: No

SENSORS BASED ON ELECTROMAGNETIC WAVELENGTHS OF MILLIMETER AND BEYOND

The use of electromagnetic waves from the millimeter and beyond is considered. One of the key issues in this wavelength range is the inability of these frequencies to penetrate conducting materials. This deficiency makes this category of detector unsuitable for field use.

Nuclear Magnetic Resonance (NMR)

NMR uses low energy photons, radio frequency (RF), to shift the magnetic moment of nucleons from one quantum state to another. The shift of the quantum state is dependent upon the nuclear structure of the atom. In medical imaging, the magnetic moment of protons is targeted for example. Two methods have been used for explosive detection:

1. Classical NMR uses a combination of RF and magnetic fields.
2. Quadrupole Resonance (QR) which uses RF alone.

Analysis of NMR

RF must be able to penetrate the material of interest. If a conductive shield such as a metal casing is present, then the RF will not penetrate. This method is not suitable for field use.

Millimeter Electromagnetic Wave (MEW)

High-resolution RADAR systems have been developed using millimeter electromagnetic waves. This type of system is useful for detecting bulk amounts of materials such as explosives. However, millimeter electromagnetic waves will not penetrate conductive materials. The inability to penetrate conductive materials makes the system unsuitable for field use.

Analysis of MEW

Since millimeter electromagnetic waves do not penetrate conductors, MEW is not suitable for field use.

METHODS THAT USE PIEZOELECTRIC EFFECTS

Gas Chromatograph/Surface Acoustic Wave (GC/SAW)

A surface acoustic wave (SAW) crystal works on the principle that a given mass of material on its surface will change its vibrational frequency. In combining a GC with a SAW crystal, the material flowing from the GC condenses on the cooled surface of a SAW crystal (see Figure 19.13). The crystal is vibrated and the frequency change of the crystal is monitored. The mass of the condensing material changes the vibrational frequency. This condensed mass is proportional to the concentration of chemical present in the atmosphere.

The GC/SAW crystal may also operate in reverse to recalibrate the system. In the reverse mode, the crystal can be heated and the condensed material boiled off.

Analysis of GC/SAW

The GC/SAW chemical sensor is a very effective method of measuring trace chemicals and has been field deployed [7]. This method has been used in detecting the chemical vapors from high explosives. Like other sensors combined with GC, it is suitable for the detection of a number of chemical vapors. Thus, it is suitable for chemical agent detection.

- Detection Time: 10 to 15 seconds
- Sensitivity: Excellent (picogram)
- Portability: Good

- Cost: Low
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

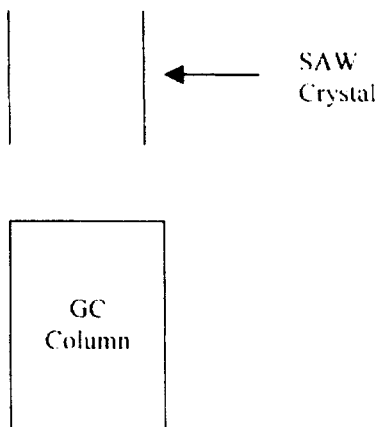


Figure 19.13 Diagram of the GC/SAW crystal.

Quartz Crystal Microbalance (QCM)

The QCM has a resonating quartz disk with metal electrodes on each side. The device has a characteristic frequency when excited by an oscillating signal. The disk is coated with a polymer that is active with sensing material. When a chemical is absorbed by the polymer, the mass of the disk increases and the resonance frequency is reduced. The QCM can see a mass change of about one picogram. This translates to a concentration of about one part per billion of the chemical agent in air.

Analysis of QCM

QCM is a well known device and has been used to measure trace amounts of chemicals.

- Detection Time: <1 second
- Sensitivity: Excellent (picogram)
- Portability: Excellent
- Cost: Low

- Data Gathering: Low
- Differentiation: Low
- Field Deployed: Yes

THERMAL TECHNIQUES

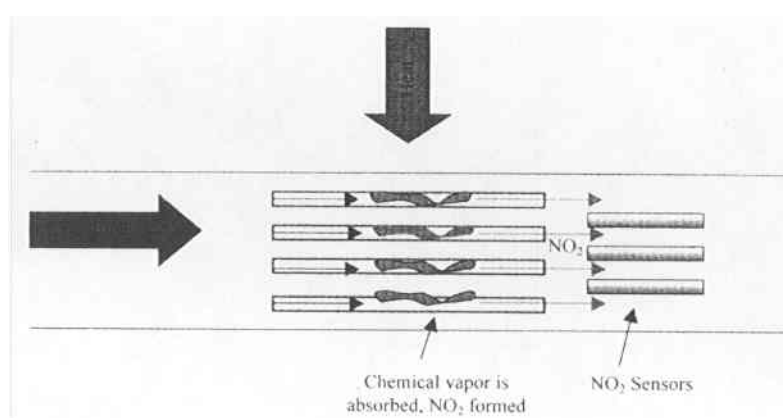


Figure 19.14 Diagram of a thermo-redox detector.

Thermo-Redox (TR)

A thermo-redox detector is similar to the chemiluminescence detector. It is basically used for the detection of explosives since it works only with nitrogen-rich materials. Air is flowed into a series of capillary tubes coated with catalytic material. The capillary tubes are heated to very high temperature. Chemical vapors from explosive materials are chemically broken down. A byproduct of this process is NO_2 . A group of sensors capable of detecting NO_2 are located at the outlet of the capillary tubes (see Figure 19.14). The signals from the NO_2 sensors are proportional to the amount of chemical vapor from high explosives that are present.

Analysis of Thermo-Redox

Thermo-redox has been field deployed for high explosives. The thermo-redox detector is not able to differentiate the type of explosive. It can detect high vapor pressure explosives like NG and TNT. It will not detect low vapor pressure

explosives like RDX and PETN. This limitation makes the thermo-redox detector unsuitable for field use.

- Detection Time: Unknown
- Sensitivity: Unknown
- Portability: Good
- Cost: Low
- Data Gathering: Low
- Differentiation: None
- Field Deployed: Yes

SURFACE EFFECT

Q-DLTS

Chemical agents have a vapor pressure. Thus molecules from a chemical agent will reach equilibrium with the surrounding air. These molecules will deposit on surfaces. A molecule absorbed by a surface will have a specific differentiable effect upon the surface potential of a material. Some materials, such as diamond terminated with hydrogen, have a low surface potential. Charge-Deep Level Transient Spectroscopy (Q-DLTS) provides information about the effect of molecules on the surface of materials such as diamond. When combined with diamond and diamond-like carbon, the technique is able to measure the quantity and type of molecule absorbed on the surface. The method is in its early stages of research but shows great promise. Initial testing has demonstrated that the method can detect and differentiate parts per billion of water vapor and ethyl alcohol in air [8]. Theoretically, the method can be orders of magnitude more sensitive than present tests demonstrate, can differentiate complex molecules and is potentially hand-sized portable.

Analysis of Q-DLTS

Q-DLTS is in early research stages but has impressive results. The technology is promising for field use.

- Detection Time: 1- to 5 seconds
 - Sensitivity: Excellent (Potentially sub-femtogram)
 - Portability: Potentially Excellent
 - Cost: Unknown but potentially low
 - Data Gathering: High
 - Differentiation: Excellent
 - Field Deployed: No
-

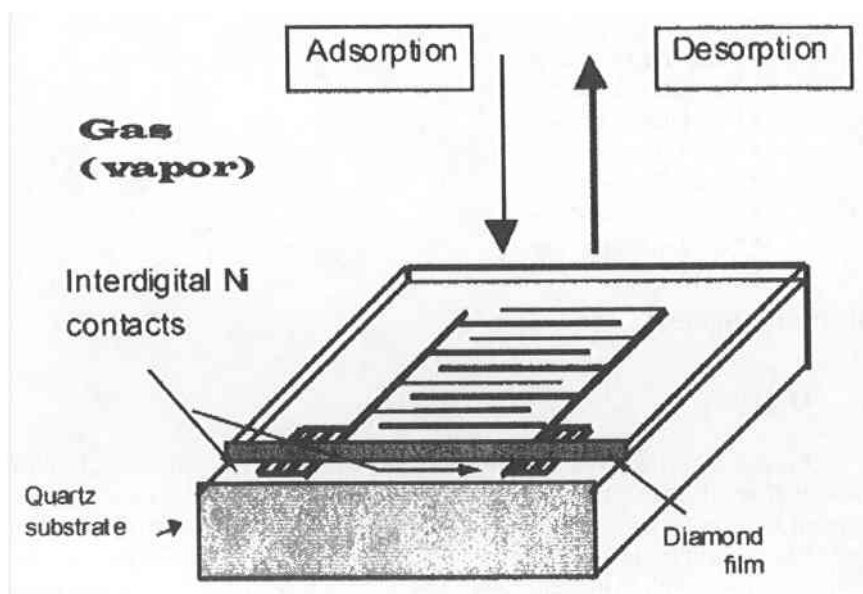


Figure 19.15 Illustration of Q-DLTS chip.

Conductivity-Based Sensors (CBS)

Changes in the resistive properties of materials like metal oxides and conducting polymer when chemicals are present on the surface can be used for conductivity-based sensors [2,9]. Unlike the Q-DLTS, in which the transient response is used, CBSs integrate the time response function and look at the real part of the surface impedance.

Analysis of CBS

CBS has been under development by organizations such as NIST for chemical detection. The surface resistances of various materials are being examined for specific chemicals. The goal of the program is to develop a database for a number of materials that respond to specific chemicals on their surfaces. These materials can be incorporated on a chip as an array of sensors that would allow the detection of multiple species. Tests have shown that metal oxide CBS sensitivity is on the order of 5 to 500 parts-per-million while the conducting polymer CBS sensitivity is on the order of 1 to 100 parts-per-million. CBSs over their lifetime will have a baseline drift.

- Detection Time: seconds
- Sensitivity: Low
- Portability: Potentially Excellent
- Cost: Unknown but potentially low
- Data Gathering: Low
- Differentiation: Moderate
- Field Deployed: No

Metal-Oxide Silicon Field-Effect –Transistor (MOSFET)

MOSFET odor-sensing is based on the principle that chemicals in contact with a catalytic metal produces a reaction in the metal. This reaction can change the electrical properties of the p-type and/or n-type materials. The sensitivity and selectivity can be varied by changing the type of catalyst, the thickness and the temperature.

Analysis of MOSFET

MOSFETs are being developed by firms in the US, France, Germany, UK and Sweden. The sensitivity of these units are about in the parts-per-million range. The units still have batch-to-batch variations. The seal on the chip's electrical connections in a harsh environment is still a problem. Finally, MOSFETs undergo a baseline drift.

- Detection Time: seconds
- Sensitivity: Low
- Portability: Potentially Excellent
- Cost: Unknown but potentially low
- Data Gathering: Low
- Differentiation: Good
- Field Deployed: No

RADIATION-BASED SENSORS

X-Rays

X-rays can penetrate materials. The penetration depth is dependent on the x-ray energy, the material thickness and the average Z (number of electrons per atom) of the material. As a group, x-ray detection systems rely on the interaction of the x-ray with matter. When an x-ray encounters matter, four things can happen:

1. The x-ray can pass through the matter unaffected
2. The x-ray can produce the photoelectric effect. An ion pair (electron plus ion) is produced.
3. The x-ray can undergo Compton scattering.
4. The x-ray can undergo pair production provided the x-ray energy is greater than 1.2 MeV.

From these interactions, it is possible to determine the density of material, the mass absorption coefficient of the material, and the effective Z of the material that the x-rays passed through. Explosives or chemical agents in bulk quantity will have unique interaction characteristics that can differentiate them from surrounding material. However, it is also possible to fool x-ray measurements by very sophisticated countermeasures. A number of x-ray systems are on the market:

- **Dual x-ray source**; which uses 75 KeV and 150 KeV x-rays simultaneously. This allows the detection of low and high-density explosives.
- **Backscatter x-ray**; which is able to see low Z objects.
- **Computer Tomography**; this method will generate a 3-D image.

Analysis of X-Ray Detection

X-ray detection has been field deployed for high explosives. The systems trigger on large amounts of explosive material with the ability to resolve shapes, density and average Z . It is possible to fool x-ray detection systems. X-ray detection systems are not suitable for field use because they work best in resolving large amounts of explosive material but not trace amounts.

- Detection Time: seconds
- Sensitivity: Poor (Needs a substantial amount of explosive: Not suitable for a trace analysis system)
- Portability: Poor
- Cost: High
- Data Gathering: Low
- Differentiation: None
- Field Deployed: yes

NEUTRON-BASED DETECTION SYSTEMS

Neutrons are much more penetrating than x-rays. Neutrons can interact with matter in the following ways:

1. Pass through the material without interaction
2. Elastic scattering (billiard ball type scatter)
3. Inelastic scattering (soft foam ball type scattering)
4. Neutron capture (results in release of radiation such as neutrons, beta particles, alpha particles, and gamma rays)

Neutron-based detection systems primarily rely on neutron capture reactions and the subsequent release of radiation. Neutron-based detection systems have a neutron source. This source can be a radioisotope such as californium (Cf) or an accelerator-based source. The neutron source is placed near the object and an array of gamma ray sensors is placed around the object. When neutrons interact with materials, some of the atoms of that material will capture neutrons. The capture reaction results in the release of gamma rays that are characteristic of the atom. The gamma ray energies and intensity are then measured. The data is sent to a computer where it is unfolded to give the density of specific atoms in the material. Additionally, some types of neutron-based detector systems can provide spatial resolution of the material. Chemical agents and high explosives are made up of chemicals. The chemicals are made up of atoms. The specific concentration of various atoms in a chemical can be determined from the gamma rays emitted from the neutron capture reaction. The density of atoms can then be related to the chemical makeup of the material through a database. Thus chemicals can be identified using neutron capture reactions.

Thermal Neutron Activation (TNA)

Thermal neutron activation uses a thermal neutron source (meaning neutron energies near the average energy of a gas molecule at room temperature, about 0.02 eV). A thermal neutron flux is made by moderating fast neutrons (meaning MeV or greater neutron energies) from an accelerator or californium source with a low Z material such as hydrogen. The thermal neutrons interact with the material of interest and neutron capture reactions take place. Sodium iodine gamma ray detectors are placed around the object and the energy and intensity of the gamma rays are measured. The data from the detectors are sent to a computer system for unfolding (see Figure 19.16).

A TNA system is commercially available from SAIC and is field deployed. It is not portable, but could be made portable with a new generation “no shielding” neutron source such as the Daimler-Chrysler Fusion Star neutron source [10].

Analysis of TNA

The TNA system is capable of probing into metal objects. This capability may be of benefit in examining trace elements inside of a sealed container. Thus TNA might be useful in the field for sealed units. TNA’s sensitivity is highly de-

pendent on the strength of the neutron source. Development of TNA for use in the field is required to sort out sensitivity issues.

- Detection Time: Minutes
- Sensitivity: ~100 gm of material depending on strength of neutron source or irradiation time.
- Portability: Poor (with Cf or accelerator source) to Good (with advanced neutron source)
- Cost: High
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

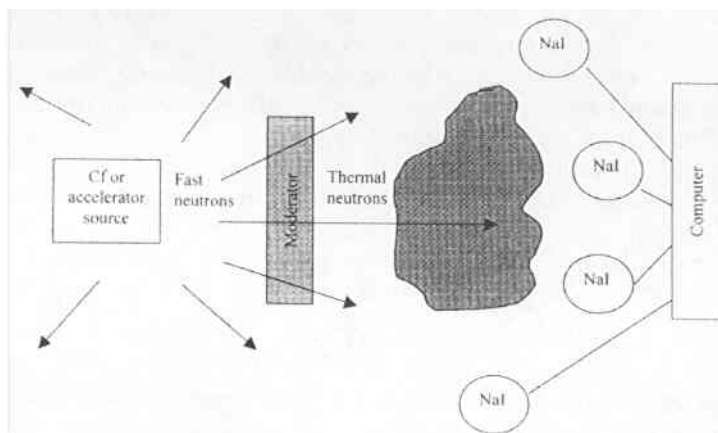


Figure 19.16 Diagram of the TNA system.

Portable Isotopic Neutron Spectroscopy (PINS)

PINS was developed by EG&G Idaho and the Idaho National Engineering Laboratory as a portable system for chemical assaying. The device uses a Cf neutron source and requires some shielding. The shielding is the main reason for the mass of the system (about 610 pounds). The device uses High Purity Germanium (HPGe) detectors but otherwise looks very much like the TNA system in Figure 22.15. Because of the HPGe detectors, this system requires a liquid nitrogen refill every 18 hours.

Analysis of PINS

PINS was designed as a portable chemical assay system. This system will be able to do chemical analysis of objects sealed in metal containers. It may be suitable for field use with sealed units. The question of PINS sensitivity for field applications must be addressed.

- Detection Time: 100 to 1000 seconds
- Sensitivity: ~100 gm of material depending on strength of neutron source
- Portability: Good (for Cf) to Excellent (for advanced neutron source).
- Cost : High
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

Pulsed Fast Neutron Analysis (PFNA)

The PFNA system is a commercial unit developed by SAIC for inspecting cargo. This system is not portable. It is large because it uses an accelerator-based neutron source ($D [d,n]He^3$) for the production of fast neutrons. The system diagram looks similar to the TNA (Figure 19.16) but PFNA has no moderator.

Analysis of PFNA

PFNA was not designed to be portable. The principle of pulsed fast neutron analysis may be useful for the field. Technology such as the Daimler-Chrysler Fusion Star may have an impact on the portability of the system. This question cannot be answered without further research and development.

- Detection Time: Sub-second
- Sensitivity: ~100 gm of material depending on strength of pulsed neutron source
- Portability: Poor, but may be improved with advanced neutron source technology
- Cost: High
- Data Gathering: High
- Differentiation: Excellent
- Field Deployed: Yes

METHODS BASED ON SURFACE WIPES (SW)

Systems such as the Expray, produced by Genesis Resource, use test paper to wipe a surface. The test paper is then treated with one of three spays:

1. Expray 1: turns dark brown-violet for TNT; blue-green for DNT; orange for TNB and picric acid.
2. Expray 2: turns pink for Semtex H, PETN, NG, smokeless powder and RDX.
3. Expray 3: turns pink with nitrates.

Analysis of Surface Wipes

Surface wipes are useful for identifying trace chemicals on surfaces. This technique may be useful in the field for checking the surface of sealed units.

- Detection Time: Seconds
- Sensitivity: Good (about 20 nanogram)
- Portability: Excellent
- Cost: Low
- Data Gathering: Low
- Differentiation: Excellent
- Field Deployed: Yes

ANTIBODY-BASED BIOSENSORS (ABB)

Immunosensors are immobilized on a solid substrate. The immunosensor is bound to fluorescently labeled signal molecules. When the signal molecules are in the presence of a specific molecule, for example RDX, the system can be designed such that the fluorescently labeled signal molecule is released. Fluorescence is then detected with a photon sensor. The photon intensity is related to the density of fluorescent molecules. The release of fluorescent molecules is then directly proportional to the chemical that is present. The construction of the sensor and reader is shown in Figure 19.17.

Analysis of Antibody-Based Biosensors

Antibody-based biosensors are under development by the Naval Research Laboratory. The technology is promising but requires more development for field applications.

- Detection Time: 1 minute
- Sensitivity: Good (1 nanogram)
- Portability: Excellent
- Cost: Unknown
- Data Gathering: Low
- Differentiation: Excellent
- Field Deployed: No

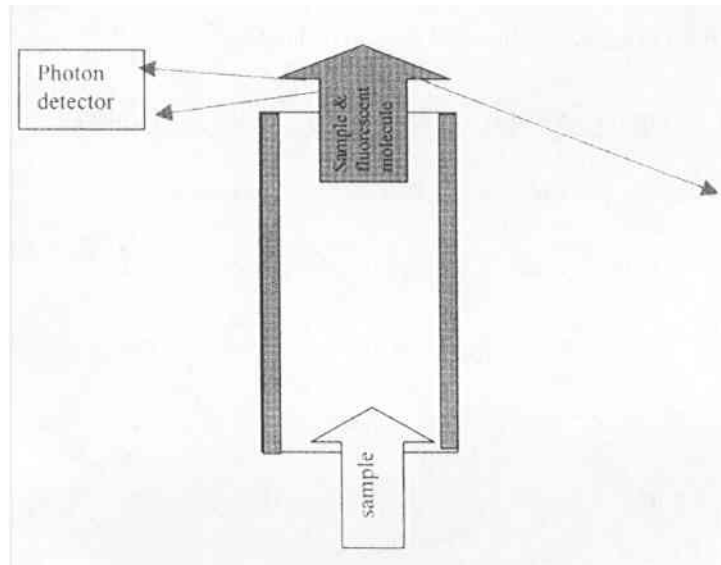


Figure 19.17 Antibody based biosensor diagram.

Antibody-Coated Oscillator (ACO)

This device uses an oscillator with a coating of antibody. As the sample flows around the coated oscillator, the chemical deposits on the antibody coating. The added mass changes the effective mass of the oscillator which changes the frequency. This change in frequency can be measured and correlates to the amount of chemical present.

Analysis of Antibody Coated Sensor

The antibody-coated sensor is very promising but the technology is still in the research phase.

- Detection Time: Unknown
- Sensitivity: Unknown
- Portability: Excellent
- Cost: Unknown

- Data Gathering: Low
- Differentiation: Excellent
- Field Deployed: No

Table 19.1 Evaluation of Chemical Sensor Technology.

Method	Time (s)	Sensitivity	Portability	Cost	Deployed
Canine	<69	Excellent	Poor	Moderate	Yes
GC	10 to 15	Good	Good	Low	Yes
ECD	<1	Good	Excellent	Low	Yes
ECD/GC	18	Good	Excellent	Low	Yes
IMS	5 to 8	Good	Excellent	Low	Yes
FIS	2	Excellent	Excellent	Low	Yes
TMS	>100	Excellent	Excellent	Unknown	No
ChL	10	Good	Good	Moderate	Yes
ChL/GC	18	Good	Good	Moderate	Yes
RS	<1	Unknown	Good	Moderate	No
OFS	<1	Unknown	Good	Unknown	No
GC/SAW	10 to 15	Excellent	Good	Low	Yes
TR	Unknown	Unknown	Good	Low	Yes
MOSFET	1 to 5	Excellent	Excellent	Low	No

Table 19.1 Continued.

Method	Time (s)	Sensitivity	Portability	Cost	Deployed
CBS	1 to 5	Poor	Excellent	Low	No
Q-DLTS	1 to 5	Excellent	Excellent	Unknown	No
TNA	>100	Poor	Poor	High	Yes
PINS	>100	Poor	Good	High	Yes
PFNA	<1	Poor	NP	High	Yes
ABB	>60	Good	Excellent	Unknown	No

The rating scale is based upon:

- Sensitivity: “Poor” indicates more than 1 part per billion or greater than 20 nanograms; “Good” indicates sub parts per billion or below 20 nanograms; “Excellent” indicates less than parts per trillion and less than a picogram.
- Portability: “NP” indicates that it is not portable; “Poor” indicates 300 to 1000 pounds; “Good” indicates 100 to 299 pounds; “Excellent” indicates less than 100 pounds.
- Cost: “Low” indicates less than \$60,000; “Moderate” indicates \$60,00 to \$299,000; and “High” indicates \$300,000 and above.
- Data Gathering: “Low” indicates not intrusive as applied to field use; “Moderate” indicates some chemicals can be distinguished as applied to field use; “High” indicates most chemicals can be distinguished as applied to field use.
- Differentiation: “None” indicates that chemicals cannot be differentiated; “Poor” indicates that only explosives can be differentiated; “Moderate” indicates that explosives and some other chemicals can be differentiated; “Excellent” indicates that most chemicals can be differentiated.
- Deployed: “No” indicates that the device has not been field deployed or tested; “Yes,” indicates that the device has been field deployed and tested.

CONCLUSIONS

The ability to measure trace chemicals in the field such as the vapor from high explosives has been demonstrated. It appears that these technologies, which were developed for security and police purposes, can be applied to many other areas including a counter terrorism tool for chemical agents.

In comparing the capabilities of chemical agent sensors with those of sensors for other agents of mass destruction, it is clear that radiation sensors are far more capable and biological sensors are far less capable.

The ultimate goal of counter terrorism is to detect the nuclear, biological or chemical agent prior to their release. Radiation sensors can detect single gamma rays or can determine the energy spectrum of gamma rays with a small number of photons. It is feasible to use radiation sensors in a pre-release mode in that these sensors can identify the radiation from nuclear materials prior to their release. Biological sensors are in their infancy and there is virtually no capability to detect biological agents prior to their release. Chemical sensors on the other hand are getting near the sensitivity required to detect chemical agents or their precursors prior to the release of the agent. Right now chemical sensors are being used to detect explosives at close proximity. Thus they can be used in situations where people are funneled to a small area such as is currently the practice in airports.

No counter measure is completely secure. For example at the time of this writing, Richard Colvin Reid, with his shoes containing plastic explosives, boarded Americans Airlines Flight 63 from Paris to Miami [11]. The only way that the plastic explosive could have been detected at the Charles de Gaulle Airport was if a bomb sniffing dog was used to check passengers, or if Mr. Reid had been asked to place his shoes on the hand luggage x-ray machine or if Mr. Reid had been stopped and his shoes wiped and tested for the residue from the explosive material. None of these were common practices at the time.

The only man-made sensor used in airports today is the residue test and it requires that the item be physically wiped. This method can detect about a nanogram of explosive material. Other types of chemical sensor technology are available that can detect sub-picograms and thus could be used to detect the vapors from explosives within close proximity. These and more advanced technologies will eventually find their way into airports and high-risk areas.

REFERENCES

1. Van Biema David, "Prophet of Poison," Time, Vol. 145, No. 14, April 3, 1995.
2. FAS, "Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo," Senate Government Affairs Permanent Subcommittee on Investigations, October 31, 1995 (http://fas.org/irp/congress/1995_rpt/aum/part01.htm).
3. Mine detection equipment, South Africa, US Army, NGIC-1142-652A-98.

4. Hannum David W. and Parmeter John E., Survey of Commercially Available Explosive Detection Technologies and Equipment, National Institute of Justice, NCJ 171133, Sept. 1998.
5. Raman Cells, 24 Hour Battle 037, Janes.
6. The How and Why of Electronic Noses, IEEE Spectrum, pp. 22-35 (September, 1998).
7. V. I. Polyakov, A. I. Rukovishnikov, A. V. Khornich, B. L. Druz, D. Kania, A. Hayes, M. A. Prelas, R. V. Tompson, T. K. Ghosh, and S. K. Loyalka, "Surface Phenomena of the Thin Diamond-Like Carbon Films," Proceedings of the Materials Research Society, V. 555, Page 345 (1999).
8. Tuttle, B. A.; Ruffner, J. A.; Olson, W. R.; Schubert, W. K.; Martin, S. J.; Mitchell, M. A.; Clem, P. G.; Dimos, D.; and Garino, T. J. "Surface micromachined flexural plate wave device integrable on silicon," Electronic Optical Materials Dep., Sandia National Laboratories, Albuquerque, NM, USA. Sandia Natl. Lab. [Tech. Rep.] SAND (1998), (SAND98-2683), 1-31.
9. Cunningham, Brian T.; Kant, Richard; Daly, Chris; Weinberg, Marc S.; Pepper, Jane Wu; Clapp, Christopher; Bousquet, Rob; and Hugh, Brenda. "Chemical vapor detection using microfabricated flexural plate silicon resonator arrays," Proc. SPIE-Int. Soc. Opt. Eng. (2000), 4036, 151-162.
10. Fusion Star, Daimler-Chrysler, x-ray free neutron source based on Inertial Electrostatic Confinement technology, Daimler-Chrysler Aerospace, Space Infrastructure Center, Trauen, Eugene-Sanger Strabe 52, D-20328, Fassberg, Germany.
11. McNeil D. G., "French Authorities Wonder: How Could It Have Happened?," New York Times, December 24, 2001. (<http://www.nytimes.com/2001/12/24/national/24PARI.html>).

BIBLIOGRAPHY

- Arnold, Neil S.; Dworzanski, Jacek P.; Muezelaar, Henk L. C.; and McClellen, William H., "Present and future challenges of developing a GC/IMS based personal chemical warfare agent detector," Editor(s): Berg, Dorothy A. Proc. ERDEC Sci. Conf. Chem. Biol. Def. Res., Publisher: National Technical Information Service, Springfield, Va., (1996), pp 653-659.
- Bryden, Wayne A.; Benson, Richard C.; Ko, Harvey W.; Donlon, Mildred; and Milton S., "Universal agent sensor for counterproliferation applications," Johns Hopkins APL Tech. Dig. (1997), 18(2), 302-308.

- Carrico, John P., "Chemical-biological defense remote sensing: what's happening," Proc. SPIE-Int. Soc. Opt. Eng. (1998), pp 45-56.
- Gittins, Christopher M.; and Marinelli, William J., "AIRIS multispectral imaging chemical sensor," Proc. SPIE-Int. Soc. Opt. Eng. (1998), pp 65-74.
- Gopalsami, Nachappa; and Raptis, Apostolos C., "Millimeter-wave imaging of thermal and chemical signatures," Proc. SPIE-Int. Soc. Opt. Eng. (1999), pp. 130-138.
- Haeber, Rainald; and Hedtmann, Joerg, "Unexploded ordnance devices: detection, recovery and disposal," NATO ASI Ser. 1 (1996), 7, pp 73-86.
- Halasz, Laszlo, "The role of remote sensing equipment in air monitoring system," NATO ASI Ser., Ser. 1 (1997), pp 241-253.
- Hannum, David W; and Parmeter, John E., "Survey of Commercially Available Explosive Detection Technologies and Equipment," National Institute of Justice, NCJ 171133, Sept. 1998.
- Holland, P. M.; Mustacich, R. V.; Everson, J. F.; Foreman, W.; Leone, M.; Naumann, W. J.; Overton, E. B.; and Carney, K. R., "Handheld GC instrumentation for chemical weapons convention treaty verification inspections," Field Screening Methods Hazard. Wastes Toxic Chem., Proc. Int. Symp., Publisher: Air & Waste Management Association, Pittsburgh, Pa., (1995), pp 229-235.
- Myasoedov, B. F., "Analytical control for destruction of chemical weapons. Requirements and organization," NATO ASI Ser., Ser. 1 (1997), pp 39-58.
- Pollina, Richard J.; and Baker, John, "DOE cooperative monitoring test bed for unattended chemical sensors," Proc. SPIE-Int. Soc. Opt. Eng. (1997), pp 254-265.
- Rider, Todd H.; and Smith, Laura., "Optoelectronic sensor," (Massachusetts Institute of Technology, USA). PCT Int. Appl. (1999), 25 pp.
- Snelson, A.; Mainer, S.; Baum, P.; and Sresty, G. "FTIR fiber-optic evanescent wave spectroscopy (FEWS) for bulk analysis of CWC-related compounds," Editor(s): Berg, Dorothy A. Proc. ERDEC Sci. Conf. Chem. Biol. Def. Res., Publisher: National Technical Information Service, Springfield, Va (1999), pp 123-129.

Swim, Cynthia R.; and Fox, Jay A., "Tunable UV and compact 2-12 micron laser development," Proc. SPIE-Int. Soc. Opt. Eng. (1998), pp 68-77.

Zardecki, Andrew; and Strittmatter, Richard B., "Chemical and isotopic determination from complex spectra," Nucl. Mater. Manage. (1995), 24, pp 817-822.

Zywicki, Randall W., "Radiometric calibration of an airborne chemical imager," Proc. SPIE-Int. Soc. Opt. Eng. (1999), pp 237-248.

20

Chemical Agents: Destruction and Decontamination

Dabir S. Viswanath and Tushar K. Ghosh

University of Missouri, Columbia, Missouri

INTRODUCTION

A number of countries have stockpiled large amounts of chemical warfare (CW) agents and other toxic chemicals and are trying to destroy them by safe methods. Factors such as cost, safety, release of secondary toxic chemicals during destruction, legal and political issues have to be considered before employing any method for the destruction of these chemicals. Although the destruction of toxic chemicals is not new and appears to have started in 1915 after the use of mustard gas by the Germans during World War I, none of the methods as we know today appear to be cost effective, safe, and foolproof. We will outline some methods used at the present time for the destruction of not only chemical weapons but other toxic chemicals. Excellent summary [1] and details [2] of several methods of destruction of toxic chemicals and munitions are available in these two citations. Heyl and McGuire [3] have edited a book entitled "Analytical Chemistry Associated with the Destruction of Chemical Weapons," which is a collection of papers presented at a NATO Workshop. This book can be an excellent resource for individuals who wish to learn more about the chemistry of destruction.

The 158 countries that have signed the Chemical Weapons Convention have agreed to destroy their chemical weapons stockpile within a certain timeframe. Table 20.1 gives an estimate of the amount of chemical weapons stockpiled by some of the countries and the schedule of destruction. However, the method of destruction to be used has not been decided yet by these countries.

The data shown in Table 20.1 also indicate the urgency of destruction of these chemical agents. If Iraq possess even 10% of CW after destruction under the

supervision of UNSCOM, it would amount to more than the current stockpiles held by Russia or the U.S.A.

The cost of destruction of CW agents is now a major issue for most of the countries that have stockpiled these agents. It is estimated that the cost of destruction of chemical weapons would be 10 times the cost of production. Renner [4], based on the information available prior to 1995, gives an excellent summary of the cost of disarmament. Further it is mentioned that the estimated cost of destruction of chemical weapons in the U.S. alone would cost \$12 billion, and the destruction of old buried chemical ammunition would cost an additional \$17.7 billion.

Table 20.1 Stockpile of chemicals [4, 5].

Country	Quantity of Chemical Weapons (tons)	Quantity of Chemical Weapons Destroyed (tons)	Destruction Cost in Billion by 2002
Russia	40,000	8000	5.7
U.S.A.	32,000	6400	9.0
Iraq*	480,000 (CW) 1,800,000 (precursors) 3,860 (1990)		
North Korea	4,500/year		
Iran	1,000/year		
India	1000		

*These figures are in liters, and represent the amount of CW and precursors destroyed under the supervision of UNSCOM. Per year figures are production capability.

DESTRUCTION METHODS

Several technologies [6] are available for destruction of toxic chemicals but most of the technologies are not cost effective. The choice of a particular technology should be based on several criteria including:

- (a) the effectiveness of the method in completely destroying the chemical,
- (b) secondary waste produced,
- (c) efficiency,
- (d) cost of destruction,
- (e) risks involved, and

- (f) broad class of compounds that can be destroyed.

Destruction of CW agents can be broadly classified into the following categories:

- Sea dumping
- Destruction by heat
- Supercritical water and wet air oxidation
- Chemical destruction

Sea Dumping

This is a method [7] practiced since World War II. This method will be suitable for chemicals that break down on hydrolysis. One major disadvantage of sea dumping is the effect of these chemicals and the hydrolysis products on marine life. This method is now prohibited by the CWC agreement, but dumping of chemicals in oceans and rivers continues to be a method of disposal of chemicals. It is estimated that after World War II 46,000 tons of chemical weapons were dumped into the Baltic Sea of which Russia dumped close to 30,000 tons. They were dumped in Baltic Sea areas known as Gotland Deep, Bornholm Deep and the Little Belt based on the information given to the Helsinki Commission in 1994 [8].

Destruction by Heat

Any chemical can be destroyed completely by applying heat. The complete destruction means that the toxic chemicals are converted to harmless chemicals such as carbon dioxide, water vapor, or nitrogen. The extent of destruction depends on the temperature of the process. Processes under this category include:

1. Incineration,
2. Pyrolysis,
3. Plasma, and
4. Molten metal technologies.

These processes are energy intensive, require special materials of construction, and the by-products can be more toxic than the precursor depending upon the temperature. Pyrolysis, plasma, and molten metal technologies require smaller vessels compared to incineration. The temperature at which each process operates varies widely from 300 K to 10,000 K.

Most of the chemicals used in chemical warfare contain heteroatoms of increased molecular complexity, and therefore processes where OH and H radicals attack the parent compound could be useful methods. These chemicals can broadly be classified as nitro- or chloro- compounds, and organophosphates.

Chemicals destroyed by these processes are nerve gases, blister agents, and other chemicals.

Incineration

In the U.S, incineration by the name of "Baseline Incineration Technology" has been used to destroy chemical warfare agents at several facilities. The Tooele Chemical Agent Disposal Facility in Utah has so far destroyed about 1,500 tons of sarin gas using baseline incineration technology. The same facility has also destroyed almost 14,000 rockets, bombs and bulk containers in the process of burning the sarin gas. The incinerator was operated at a temperature of 1750 K, and the products of incineration are sent to a second incinerator or afterburner for complete combustion of even the traces coming out of the first incinerator. The baseline incineration process used at Johnston Atoll destroyed chemical agents in the weapons stored there with an efficiency of 99.9999 percent [9]. Several more incinerators are under construction by the US military so that the CWC treaty's deadline for destruction of chemical warfare agents can be accomplished. Several modifications to the original baseline incineration technology were proposed. A Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, Board on Army Science and Technology by National Research Council has reviewed these modifications [9]. The baseline incineration system is so named because it was initially the Army's preferred method for destroying chemical agents and assembled chemical munitions. The modified baseline process is distinguished from the baseline incineration system in that both the mustard agent and munition body are fed to one furnace instead of being separated and sent to different furnaces. This modification is intended to solve the problem of gelled agent that has formed in the aging munitions and cannot be drained from the munition body. Preliminary testing has shown that the chemical agents in the weapons stored can be destroyed with an efficiency of 99.9999 percent.

Incineration is a widely used and proven technology with a long history of research and development. The chemistry of the destruction process and conditions for effective operation are well established. This improved understanding has been developed during the past few years and, because of facilities improperly operated in the past, incineration suffers from a poor public image. In the US, Center for Disease Control's National Center for Environmental Health (NCEH) reviews all Department of Defense (DOD) plans for disposing of chemical weapon stockpiles. DOD incinerators must meet all the local, state, and federal standards for a variety of emissions and must achieve a "destruction and removal efficiency" of 99.9999% for the agent being destroyed. This means that no more than 0.0001% of the agent being processed can be released from the incinerator stack. Instruments continuously monitor the incinerator stack for the agent at extremely low levels, well below levels considered safe for the community. If any agent is detected in the incinerator stack, the incinerator automatically shuts down until problems are corrected. Quality control specialists check agent-monitoring instruments in the stacks and elsewhere in the workplace each day. NCEH reviews

all agent-monitor quality control reports biweekly to ensure that workers operate the monitors in accordance with standard practices and with site-specific procedures that NCEH helped to develop [10].

Pyrolysis

Chemical agents like nerve agents and, possibly, mustard compounds can be destroyed by the pyrolysis (thermal treatment without oxygen) process. A number of other toxic organic compounds can be also destroyed. The advantage of the pyrolysis process compared to incineration is that for the same amount of materials, pyrolysis requires smaller reactors, no mixing, and lower temperatures. However, pyrolysis may produce toxic byproducts which still have to be destroyed by some other processes. If incineration is used, pyrolysis is often the first step in the multi-step destruction process.

Plasma-Based Destruction

In this process a plasma arc generates temperatures around 3000 to 10,000 K. At this temperature chemicals break down into atoms or fragments containing few atoms. The reactions proceed very fast at very short residence times. Although a commercial scale unit using plasma-based thermal destruction system for chemical agents is not available, the process has been tested in pilot scale by several companies for destroying other wastes. Westinghouse has tested plasma vitrification technology for high-level and low-level nuclear waste. In this process calcination and vitrification are integrated into a single process. Bruce et al. [11] reported development of a plasma-based thermal treatment process for destroying polychlorinated biphenyls (PCBs) and chemical warfare agents. Testing was conducted using simulants for chemical and nerve agents and other energetics. Destruction and removal efficiencies in the range of >99.9999% were reported.

Molten Metal Systems

Molten Metal systems use a heated bath, typically of Fe or Ni to destroy the chemicals. However, such systems require an off-gas treatment facility. Carry over of particulates with the off gas and the life of the refractory materials used to line the vessel are of great concern. Treatment of wastes using an enclosed molten metal system includes the possibility for the production of useful chemicals, such as syngas ($\text{CO} + \text{H}_2$), from the decomposition chemistry in the bath. This technology may also find use for treatment of wastes containing metals; for example arsenic may be captured.

Supercritical Water and Wet Air Oxidation

Supercritical Water Oxidation and Wet Air Oxidation processes operate at temperatures above 700 K and high pressures up to 250 – 300 bar. Water is used as the supercritical fluid. Although this method requires high pressure and special

materials of construction, it has an added advantage that other oxidants such as oxygen, hydrogen peroxide, or any other compound can be used to increase the efficiency of destruction and to reduce the production of other toxic wastes. Los Alamos Laboratory has designed and built a high pressure system for the destruction of explosives. It has a capacity of 400 liters/day and is made out of inconel and titanium.

The feed stream is generally in the liquid form. Insoluble liquids and solids have to be processed in the form of slurries. Although pure oxygen is the best source of oxidant, compressed air can also be used. Hydrogen peroxide is another oxidant, but is more expensive.

General Atomics Corporation is building a 4000 L/day SCWO mobile reactor for propellants and chemical weapon agents. They report having successfully treated GB, VX and mustard on the laboratory scale. The cost to build a unit running 20 L/min is \$2,000,000.

Chemical Destruction

Chemical methods for destruction of chemical agents are a good alternative to energy intensive high temperature processes, and high pressure wet air oxidation or supercritical water oxidation processes. These methods include:

1. Neutralization
2. Hydrogenation
3. Hydrochlorination

Neutralization

One method of chemical destruction is by neutralization [12]. The US Army has successfully carried out the destruction of nerve agents such as GB and vesicants such as mustard gas using alkali treatment. However some disadvantages of this process are large amounts and type of the waste products, cost of operation, analysis of complex mixtures to certify complete destruction of the toxic chemicals, and safety.

Hydrogenation

A second chemical method of destruction of chemical agents is by hydrogenation. This process can be used for chemicals like mustard gas but may not be suitable for nerve agents. However, Eco Logic Solutions [13] report that their gas-phase chemical reduction process is capable of destroying in excess of 99.99% of VX and sulfur mustard. This process needs proper catalysts and produces hydrogen sulfide and hydrochloric acid gas as products. Although several methods have been tested for the destruction of explosives, very few methods have been tested for toxic chemicals like nerve gases. A hydrogenation reactor under standard conditions runs at about 1 bar with three fold excess hydrogen and needs about 1-10

seconds of reaction time. The reactor temperature for halogenated hydrocarbons is about 850 °C.

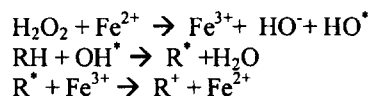
Hydrochlorination

Yet another chemical destruction method is hydrochlorination wherein dry hydrochloric acid gas is used to react with nerve agents. This method is not expected to produce toxic products, and could be carried out at temperatures between 420 to 520 K.

Advanced Oxidation Processes

Advanced Oxidation processes are other alternative methods, and several variations can be researched based on method of free radical formation. Some of the processes in this category are ozonation, Fenton's reagent, TiO₂ catalysis, and Electrochemical peroxidation.

Electrochemical processes depend on Fenton's reaction which creates free radicals. The mechanism is complex but one scheme is:



RH is the organic molecule, and if the reaction is carried to completion, it is expected that the organic molecule breaks down into CO₂ and water. The current status of these technologies is summarized in Table 20.2.

EQUIPMENT DECONTAMINATION

The objective of decontamination is to rapidly and effectively remove poisonous chemical agents both from personnel and equipment to avoid secondary contamination. Decontamination of personnel of chemical agents has been discussed in Chapter 18. In this section only decontamination of equipment and other exposed surfaces are discussed. Decontamination is time-consuming and requires resources, therefore, contamination should be avoided to the extent possible. Some simple measures may be taken to avoid heavy contamination. Equipment can be covered, for example, or easily decontaminated equipment can be chosen by means of suitable design and resistant surface cover.

However, it may be noted that some chemical agents such as nerve agents are highly soluble in paint, plastics and rubber, making their surface decontamination a difficult task. Similarly, chemical agents can penetrate various materials and remain there undecomposed for a long period of time. The slow decomposition will result in a release of toxic gases for a long period of time. The level of clean up will depend on the regulatory requirement or health concern.

Table 20.2 Summary of process capabilities and status [2].

Process	Stream Treated					After - burner Needed	Next Step	Comments
	Agent		Need Gas Afterburner	Metal and Energetics				
	Initial Agent Detox	Complete Organic Oxidation		Energetics	Metal			
<i>Low temperature, low Pressure detoxification</i>								
Base hydrolysis	GB	No	?	No	No	N.A.	PP	Has been used in field for HD, Limited by contacting problems
NaOH+H ₂ O ₂	VX	No	Yes	No	No	N.A.	Lab	New finding
Ca(OH) ₂ at 100°C	HD	No	?	No	No	N.A.	Lab/PP	Limited use in England
KOH+ethanol	HD, GB, VX	No	?	No	No	N.A.	Lab	
Hypochlorite ion	HD	No	Yes	No	No	N.A.	Lab	Difficult contacting problem with HD
Organic base (ethanolamine)	GB, HD, Possibly VX	No	?	No	No	N.A.	Lab/PP	Limited use in Russia; increase in organic use

Table 20.2 (continued).

Process	Stream Treated					After- burner Needed	Next Step	Comments
	Agent		Need Gas Afterburner	Metal and Energetics				
	Initial Agent Detox	Complete Organic Oxida- tion		Energetics	Metal			
<i>Acidic Systems</i>								
HCl Hydrolysis	GB	No	?	No	No	N.A.	Lab/PP	
Peracid salts (OXONE, others)	VX, perhaps GB and HD	No	Yes	No	No	N.A.	Lab/PP	Increased waste
Chlorine	VX, perhaps HD and GB	No	Yes	No	No	N.A.	Lab/PP	Increased inorganic waste
Ionizing radiation	All	No	?	Yes?	Yes?	?	Lab	High conversion not yet established
<i>Low temperature low pressure oxidation</i>								
Peroxydisulfate, ClO ₃ , H ₂ O ₂ , O ₃	All	Yes	Yes	No	No	N.A.	Lab	Catalysts generally needed for complete conversion; spent peroxydisulfate can be electrochemically regenerated

Table 20.2 (continued).

Process	Stream Treated					After- burner Needed	Next Step	Comments
	Agent		Need Gas Afterburner	Metal and Energetics				
	Initial Agent Detox	Complete Organic Oxida- tion		Energetics	Metal			
UV light with O ₃ and H ₂ O ₂	N.A.	Yes	Yes	No	No	N.A.	PP	Very large power re- quirement, applica- tions have been for very dilute solutions
Electrochemical oxidation	All	Yes	Yes	No	No	N.A.	Lab	
Biological oxida- tion	N.A.	Yes	Yes	No	No	N.A.	Lab	
<i>Moderate tem- perature, low pressure oxida- tion</i>								
Wet air and super- critical water oxidation	All	Partially	Yes	Yes?	No	Yes	PP	Residual organic com- ponents can be low for supercritical, re- sidual materials are believed suitable for biodegradation

Table 20.2 (continued).

Process	Stream Treated					After- burner Needed	Next Step	Comments
	Agent		Need Gas Afterburner	Metal and Energetics				
	Initial Agent Detox	Complete Organic Oxida- tion		Energetics	Metal			
<i>High temperature low pressure py- rolysis</i>								
Kiln (external heat)	All	Partially	Yes	Yes	Yes	Yes	Demo	May need more than one unit to deal with all streams
Molten metal	All	No	Yes	Yes?	Yes	Yes	PP	
Plasma arc	All	No	Yes	Yes?	Yes	Yes	Lab/PP	
Steam reforming	All	Yes	Yes	No?	No	Yes	Lab/PP	
<i>High temperature low pressure Oxidation</i>								
Catalytic, fixed bed	N.A.	N.A.	N.A.	No	No	No	Lab/PP	Useful for afterburner
Catalytic, fluid- ized bed	All	Yes	Yes	Yes	No	Yes	PP	
Molten salt	All	Yes	Yes	Yes?	No	Yes	Pp	Possible use for after- burner and acid gas removal

Table 20.2 (continued).

Process	Stream Treated						Next Step	Comments
	Agent		Need Gas Afterburner	Metal and Energetics		After-burner Needed		
	Initial Agent Detox	Complete Organic Oxidation		Energetics	Metal			
Combustion Other Technologies	All	Yes	Yes	Yes	Yes	Yes	Baseline technology	
Hydrogenation	All	No	Yes	No	No	No	Lab	
Reaction with sulfur	All	Yes	Yes	No	No	No	Lab	

Note: Question mark (?) indicates uncertainty about the noted application. N.A.: Not applicable; PP: pilot plant; Demo: demonstration;

Lab: laboratory

As noted by Raber et al. [14] dose information for a number of potential chemical agents is not available or controversial. Environmental regulatory limits or health guidelines are necessary to establish clean-up concentration level. Therefore the key issues prior to decontamination of a site or equipment are to determine exactly what constitutes a safety hazard and whether decontamination is necessary for a particular scenario. Also it should be kept in mind that the need and extent of decontamination can only be established by means of detection. If detection is not possible, then decontamination must be done solely on suspicion of contamination, e.g., if the unit has passed on the fringe of a contaminated area. Also the detection limit of the instrument should be taken into consideration when calculating or assessing health risks.

All decontamination is based on one or more of the following principles [15]:

- to destroy CW agents by chemically modifying them (destruction),
- to physically remove CW agents by absorption, washing or evaporation,
- to physically screen-off the CW agent so that it causes no damage.

Most chemical agents can be destroyed using other chemicals. However, a single chemical or a chemical mixture is not available that is effective against all types of agents. The decontaminating chemicals can be corrosive to surface or may remain in the environment creating a secondary problem.

Equipment can be decontaminated by washing and rinsing them with water containing additives such as detergents, soap, paraffin and carburetor spirit. Emulsified solvents in water can be used to dissolve and wash off the agents from equipment. Heat treatment is another option for removing or evaporating agents from equipment surface; however, it may not be convenient particularly if the size is too large. The hot water or steam may be used as a heat source if heat treatment is deemed necessary.

Chemical agents can easily penetrate various materials and into crevasses. The water rinsing alone cannot remove the agents from the equipment. When an agent has penetrated into the surface, it is necessary to use a deep-penetrating solution. If such a method cannot be used, the equipment cannot be used for a long period. In those scenarios, the equipment should be left alone for "self-decontamination." The time necessary for self-decontamination is shown in Table 20.3. This may take many days or even weeks. The absorption into the surface and natural chemical degradation are important factors influencing the self-decontamination period. The penetration ability of a CW agent can be enhanced when mixed with solvent. Chemical warfare agent resistant paints and materials may be used to protect these equipment, which implies that water-based methods will become more effective. However, such types of paints or materials are still in the development stage. A modern decontaminant is the German Münster emulsion which consists of calcium hypochlorite, tetrachlorethylene, emulsifier ("phase

transfer" catalyst) and water. Instead of tetrachlorethylene, the more environmentally harmless xylene is sometimes used.

Table 20.3 Self-decontamination times for contamination on metal surfaces and on a typical (non-resistant) paint at + 15 °C, 4 m/s, and 2 mm large droplets [15].

Substances	No contact risk	
	Liquid	Gas
<i>Untreated metal surface</i>		
Soman	< 5 h	< 5 h
Mustard agent	< 20 h	< 20 h
VX	6-8 days	6-8 days
<i>Painted metal surface</i>		
Soman	3-4 h	1,5 days
Mustard agent	1 day	3 days
VX	6 days	12-15 days

Note. The times for "liquid" only indicate when the surface is free of liquid, e.g., no liquid is transferred when touched. There is still a risk involved in contact and inhalation through release of gas from surfaces where the CW agent has penetrated deeply.

When decontaminating by washing, the subsequent treatment of contaminated liquid must be considered. The solution will contain trace amounts of these chemical agents and therefore need further treatment before discharging to the environment. However, often the additives present in the rinse liquid can destroy some the agents making discharge of the washing liquid easier. When washing with hot water and detergent, the CW agent will often be decomposed to some extent through hydrolysis. Detergents containing perborates are particularly effective in destroying nerve agents. Without an addition of perborates in the detergent, the hydrolysis products of V-agents may still remain toxic unless the pH is sufficiently high. Mustard agent is encapsulated by the detergent and, consequently, the hydrolysis rate decreases in comparison with clean water. However, the low solubility of mustard agent makes it difficult to remove without the addition of detergent, but the water used will still contain undestroyed mustard agent.

Small areas of terrain or a contaminated site may be decontaminated by removal of the top-soil followed by incineration of the soil or through self decontamination. In the case of self-decontamination, the soil should be isolated and care must be taken to prevent leaching out due to rain. Another alternative is to cover the soil with chlorinated lime powder (sludge), which releases active chlorine slowly over a long period of time. The released chlorine vapor can react with the CW into the soil and destroy them eventually.

A contaminated site can be also covered with a layer of soil or gravel preventing direct contact with the chemical agents. However, this can only be considered a temporary solution. The chemical agent will break down or decompose over time and release toxic vapor that can diffuse through the top layer into the atmosphere and recontaminate equipment. The effect will be improved if bleaching powder is mixed into the covering material. However, this can create a corrosive environment.

Various other techniques have been explored for rapid decontamination of equipment. The Safety Equipment Development AB of Sweden has developed a decontamination tent for decontamination of personal equipment and lighter articles. The tent is heated with a mixture of hot exhaust gases and air from a small jet-pulse engine. The temperature in the tent is kept at about 130°C and in the container at 80-130 °C, depending on the type of material to be decontaminated. Decontamination time varies between two and five hours depending on the temperature.

Decontamination of vehicles and other large objects sometimes is done with steam and suspension and/or emulsion systems. Alfred Karcher GmbH & Co./VPS of Germany has developed a special equipment, C8-DADS (Direct Application Decontamination System), in which the emulsion is prepared and then dispersed onto the vehicle or the terrain.

Sandia National Laboratory (SNL) in the US is developing a decontaminating foam for destroying chemical agents [16]. Several tests were conducted with chemical agent simulants. The chemical agent simulants used were diphenyl chlorophosphate (simulant for G-agents), 2-chlorethyl phenylsulfide (simulant for H-agents) and O-ethyl-S-ethyl Phenylphosphonothioate (simulant for VX). Testing was done via solution tests where the agent was added to the decontamination foam and surface tests in which the agent was placed on a surface which was then exposed to the foam. The decontamination foam did not generate any toxic or hazardous by-products.

Tests were also conducted using actual agents. The test results for foam decontamination of paper with GD, VX, and HD are given in Figure 20.1. The half-lives for the decontamination of these CW agents by the foam is on the order of 2 minutes to 15 minutes.

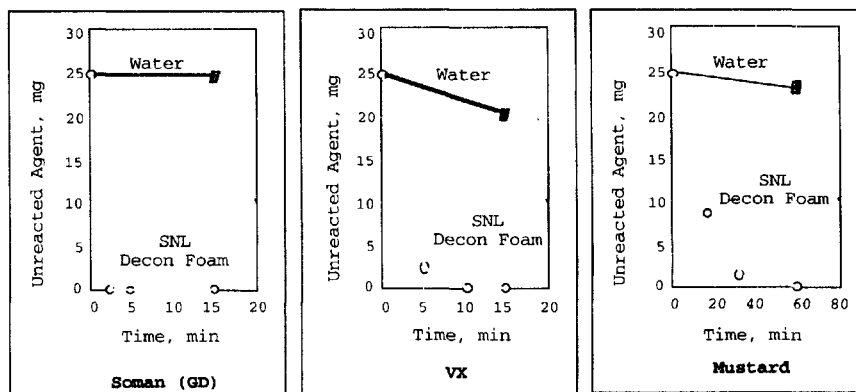


Figure 20.1 Decontamination of paper treated with chemical agent at 25mg/25 cm². Foam was applied on contaminated paper for a given duration. Residual simulant on the paper and in the foam were determined by GC and added to determine total unreacted agent [16].

REFERENCES

1. RW Shaw, MJ Cullinane, in "Destruction of Military Toxic Materials" in The Encyclopedia of Environmental Analysis and Remediation, Vol.8, R.A. Meyers, Wiley, New York, N.Y., 1998. <http://www.aro.army.mil/chemb/people/milremed.html>
2. Alternative Technologies for the Destruction of Chemical Agents and Munition, NRC, National Academy Press, Washington, D. C., 1993.
3. M Heyl, R McGuire, Eds. "Analytical Chemistry Associated with the Destruction of Chemical Weapons," Kluwer Academic Publishers, Hingham, MA., 1997.
4. M. Renner, Bonn International Center for Conversion, Brief 6, Bonn, Germany, 1996.
5. AE. Smithson, The Bulletin of Atomic Scientists. April 1993 NTI: Country Overview.
6. Disposal of Chemical Weapons: Alternate Technologies, Congress of the United States, Office of Technology Assessment, 1992.
7. M Bowers. The disposal of surplus chemical weapons. Chapter 3. In Coping with Surplus Weapons: A Priority for Conversion Research and Policy. EJ laurance. H Wulf. Eds. (<http://www.bicc.de/weapons/brief3/chap3.html>), April 16, 2002.
8. Report of the Nato Advanced Research Workshop on Destruction of Military Toxic Waste, Naaldwijk, The Netherlands, 22-27 May 1994.

9. A Modified Baseline Incineration Process for Mustard Projectiles at Pueblo Chemical Depot Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, Board on Army Science and Technology, National Research Council. National academy press, Washington, D.C., 2001.
10. Demilitarization of Chemical Weapons: How Safe are Incinerators? (CDC Brochure) <http://www.cdc.gov/nceh/demil/brochures/demilfaq.htm>
11. KR Bruce, J Lee, D Freed, L Heredy. Evaluation of a plasms-based thermal treatment system for destruction of difficult to remediate wastes. Proc of the International Conference on Incineration and Thermal Treatment Technologies. Salt Lake City, May 11-15, 1998.
12. Bechtel National, Inc. and US Army Program Manager for Cooperative Threat Reduction (PM-CTR), Joint evaluation of the Russian two-stage chemical agent destruction process, final technical report: phases 1 & 2 (revised July 1996), p. xii; 4
13. Eco Logic's gas-phase chemical reduction process. (<http://www.eco-logic-intl.com>).
14. E Raber, A Jin, K Noonan, R Mcguire, RD Kirvel. Decontamination issues for chemical and biological warfare agents: How clean is clean enough? International Journal of Environmental Health Research. 11(2): 128-148, 2001.
15. Decontamination of Chemical Warfare Agents. An Introduction to Methods and Chemical for Decontamination. www.opcw.nl/chemhaz/decon.htm.
16. SNL Decon Formulation for Mitigation and Decontamination of CBW Agents. Decontamination Performance for Chemical Agent Simulants. www.nwmp.sandia.gov/SNLdecon/demos/demo1.htm.

21

Chemical Agents: Threats and Countermeasures

L. David Ormerod, Tushar K. Ghosh, and Dabir S. Viswanath

University of Missouri, Columbia, Missouri

INTRODUCTION

In the Twentieth Century, the propagation of chemical warfare and its defense were strategic considerations of most major and many secondary powers. The seminal introduction of mass chemical attack occurred near Ypres in Belgium on April 22, 1915 when German Army forces released 180 tonnes of chlorine gas upon French, Algerian, and Canadian positions. Respirator protection was devised as protection against inhalation of these new chemical weapons (CW). In 1916, the British Expeditionary Force introduced phosgene and chloropicrin, and the French introduced hydrogen cyanide. In 1917 (also near Ypres), the first use of mustard agent by Germany inaugurated a CW with marked cutaneous reactivity and systemic absorption via the skin, thereby markedly increasing the complexity of CW warfare and its defense. Despite the widespread use of CW in World War I with 1.3 million CW casualties and 90,000 deaths, their role remained principally tactical.

Subsequently, chemical warfare was utilized in military operations in Morocco (1923-26), Libya (1930), Sinkiang (1934), Ethiopia (1935-40), China (1937-42), Vietnam (1961-75), Yemen (1963-67), and in the Iran-Iraq war (1980-88) [1]. However, although extensive stockpiles were developed in World War II, chemical weapons were not used by either side, perhaps because of a combination of high quality defensive measures and the risks of massive military retribution.

The principal method militarily of disseminating chemical weapons has involved the use of explosives to distribute the agent. Aerodynamic distribution controls particle size and enhances dispersion, but the altitude of dissemination,

wind speed, and direction are more critical [2]. Many munitions are designed to detonate 200 to 300 feet above ground level. State-sponsored terrorists might gain access to military grade CW, but other groups may have to either manufacture their own, adapt commercially available chemicals as weapons, or cause chemical releases from commercial sites or transporters.

WHITHER CHEMICAL WEAPONS DISARMAMENT

Chemical weapons have failed to demonstrate crucial strategic capabilities against protected military forces. The widespread proliferation of chemical weapons with greatly increased destructiveness and the development of increasingly sophisticated munitions was countered by effective protective measures and by sensitive means of detection (see Chapter 19). The visceral opprobrium of civilian populations, notably in the USA and Europe, led to widespread perception that the risks from such weapons exceeded the potential military benefits. Moreover, the increasing complexity of post-cold war international relations and the proliferation of CW technology to certain developing countries, supportive of asymmetric conflict for perceived international inequities, created new risks for the international community of nations from state-sponsored CW terrorism. Because of customary military secrecy and the especial governmental sensitivities associated with ethical ambivalence over chemical weaponry, a high degree of technical sophistication has been required of the many diplomatic negotiators and policy makers involved over the last century of CW disarmament [3].

In 1874, the Brussels Convention on the Law and Customs of War prohibited the use of poison or poisoned weapons and the use of materiel to cause unnecessary suffering. The 1899 Hague Convention formally proscribed the use of projectiles containing chemical weapons, but was proven ineffective by World War I in which 190,000 tons of CW were deployed. The League of Nations approved the 1925 Geneva Protocol (for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare), but which retained the right to develop, manufacture, and stockpile CW for defensive purposes. The US was a signatory but did not ratify the treaty until 1975, and retained the right to self-defense and first-strike deterrent uses of CW. Armed CW deterrence proved largely effective in World War II, despite the absence of detection and enforcement provisions within the Geneva Protocol.

The massive Soviet Union post-war CW program was countered with large US CW munition stockpiles, and paralleled by many developed nations. Several countries including US and Russia have formally acknowledged possessing CW although about two dozen countries were believed to possess a CW program. The increasing dissemination of CW to the developing world and CW use in regional conflicts was countered by the Australia Group of nations, who devised a voluntary system of controls on the export of CW precursor chemicals from the primary producing nations. This was organized through the Organization for Economic

Cooperation and Development (OECD), but export controls proved only partially successful.

President George Bush Sr. arranged a bilateral CW stockpile reduction agreement with the Soviet Union in 1990, followed by the unilateral declaration of US CW disarmament in 1991. International diplomatic negotiations that had been proceeding progressively for 20 years were put on the fast track by these commitments, resulting in the final formulation of the Convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and on their Destruction. The Chemical Weapons Convention was finally signed by the 65 countries required for ratification in 1993, and there are currently 145 countries that have ratified or acceded to the treaty. For the first time in a disarmament agreement, the multilateral regime provided for extensive on-site verification and investigation in an attempt to assure the comprehensive destruction of CW stockpiles and of CW manufacturing plants, oversight of the use of certain precursor chemicals, redress of treaty violations, and mutual assistance in the event of attack or threat of attack, including CW terrorism.

The Organization for the Prohibition of Chemical Weapons (OPCW), headquartered at the Hague in the Netherlands, is the international authority for the 1993 Convention, and comprises an international bureaucracy of approximately 500 individuals, including 200 inspectors, charged with organizational, executive, and technical verification functions. Among the inspection regimes are short-notice targeted compliance inspections and the placement of on-site remote monitoring devices. The goal is to supervise the global destruction of all chemical weapons over a 10-year period from the 1997 date of implementation.[4]. The CW Convention is the first treaty to ban an entire category of weapons under stringent international inspection.

Seventy different chemical weapon agents were stockpiled during the 20th century, but many failed to stand the test of time. Table 21.1 breaks down the aggregate total of 69,893 metric tons of weaponized chemicals declared to OPCW by its member states as of December 31, 2000 [5]. Six thousand seven hundred metric tons had been destroyed as of April 1, 2002 comprising 2 million of the 8.6 million items awaiting destruction [6]. The US stockpile is the second largest after Russia and consists mainly of nerve gas (GB and VX) and vesicants (primarily mustard agents: H and HD). Approximately 60% of the US stockpile is in bulk storage containers, and 40% is contained in munitions - of 150,000 gross tonnage. Among the worldwide chemical armaments to be destroyed are ballistic and cruise missile warheads, artillery shells, mortars, grenades, landmines, aircraft bombs, spray tanks, and binary munitions (in which the precursors are combined on firing). Destruction of US weapons is occurring by incineration at Johnston Atoll, 250 miles southwest of Hawaii, and by chemical neutralization at a Utah facility.

The road to worldwide chemical weapon disarmament remains an uncertain if hopeful journey of multilateral international cooperation. There has been significant opposition within the executive and legislative branches of the US government to the more burdensome monitoring requirements and because of an alleged

necessity to protect industrial-secrets, despite the strong support for the treaty by the Chemical Manufacturers Association and the American Chemical Society. Subsequently, Washington sought special considerations, including a presidential veto over challenge inspections, and orchestrated the premature replacement of the OPCW Executive-Director, leading to accusations of unilateralism and concern over the potential creation of loopholes for CW 'cheaters.'

Several US objections have been raised to the Convention [7]. There is a mistaken assumption underlying most of these objections that CW are generally a weapon of mass destruction. The manifest demonstration of overwhelming remote strike capability of US forces with the utilization of 'smart' munitions in the recent Afghanistan, Kosovo, and Iraq conflicts undermines the argument that a specific CW deterrent is necessary if nuclear weapon deterrence is not to be made more likely. The necessary detailed verification provisions and advances in chemical detection will make the identification and cessation of major CW programs verifiable, for the first time. The treaty mandates the acceptance of short-notice challenge inspections at any suspect site within the nation state. Small-scale noncompliance might indeed remain undetected. However, to conventional munition deterrence and military superiority of the US and its allies is added the demonstrated mutual interests of the comity of nations in the abolition of CW. Defensive measures against the use of CW would remain unaffected.

Of the more than 2 dozen countries possessing CW, only North Korea, Israel, Syria, Egypt, Iraq, and Libya remain outside the Convention; Iran, Pakistan, and Sudan have enjoined the treaty [8]. Even without universal compliance, the Convention should markedly reverse the proliferation of CW, and the risks of terrorist acquisition, and provide the framework for international economic, political, and possibly military pressure upon noncompliant 'rogue states' seeking to maintain CW programs. The alternative of widespread proliferation of CW among states would make their eventual acquisition by terrorist groups very much more likely [9].

RISK ANALYSIS OF THE POSSIBILITY OF CHEMICAL WEAPON ATTACKS ON US CIVILIANS

It is perhaps unlikely that a terrorist group would ever be able to obtain munition weapons, particularly since the advent of international CW disarmament activities under the Chemical Weapons Convention (1993). There has been concern that the poor security of stored CW agents in several countries of the former Soviet Union and sales from stockpiles left over from the Iran-Iraq war of 1980-88 might result in a market for chemical weapons among terrorist groups. This situation has improved with the cooperation of governments and with US employment-subsidization of former Soviet government scientists with chemical (or biological) weapon expertise. Unease remains that so-called 'rogue states,' such as Iraq, North Korea, Syria, Israel, and Libya, who maintain covert chemical weapons programs

and whose stockpiles are undeclared to the OPCW [1] might disseminate weaponized chemicals to terrorist organizations. There is no objective evidence that this has occurred [10]. The risks would certainly change if nation states become directly involved, but detection would lead to international opprobrium/and the likelihood of massive retaliation.

Table 21.1 Aggregate Quantities of Chemical Weapon Agents Declared to the Organization for the Prohibition of Chemical Weapons (OPCW), December 31, 2000.

Category 1 Chemical weapons	Total tonnage
Lewisite (L)	6,745
Mustard/Lewisite mixtures	344
Mustard agent	13,839
Runcol (HT) [mustard 60% + Agent T 40%]	3,536
Degraded sulfur mustard	1
Tabun (GA)	2
Sarin (GB)	15,048
Soman (GD)	9,175
Medemo	<1
Agent VX	4,032
Agent VR	15,558
Difluor (DF) {binary}	444
OPA {binary}	731
EDMP {binary}	46
Unknown	4
Category 2 Chemical weapons	
Chloroethanol	302
Thiodiglycol	51
Phosgene	5

Source: Health Aspects of Biological and Chemical Weapons, WHO, 2002
American military CW nomenclature is included [5].

The question therefore arises as to the magnitude of the risk that international or national terrorist organizations could manufacture, store, and disperse their own chemical weapons in the US. Extensive national and international law now exists to regulate access to precursor chemicals and to certain manufacturing

equipment. Still, many precursor chemicals and much equipment is dual-use and readily available commercially. There are, moreover, major constraints in the fairly sophisticated scientific skills and specialized manufacturing equipment necessary to manufacture, in safety, most of the recognized CW agents. Such constraints are commonly underestimated in political and journalistic commentaries. For a terrorist organization to make considerable technical and financial investment in developing unconventional chemical weapons, and to undertake the prolonged acquisition process, with the potential for detection, there will have to be a strategic advantage identified. The regular tools of the terrorist trade are much easier to acquire and use, and would be expected to serve their purposes at least equally as well. In the open air, for example, it is estimated that approximately 1,000 kg of sarin would be necessary, if expertly deployed, to exceed the potential of conventional explosives. Unless there is direct state or proxy support of CW acquisition or development, large-scale use of CW by non-statal protagonists is unlikely. Improved US intelligence capabilities are also a potent disincentive.

However, the manufacture of a variety of chemical weapons by Aum Shinrikyo and the 1994 sarin attacks on the judges' compound in Matsumoto and on the Tokyo underground in 1995 brought into clear focus that a determined civilian group with extensive financial and scientific resources could actually threaten a sovereign state [11, 12]. There were also failed attacks with botulinum toxin and failed biological weapon attacks. The potential for mass civilian casualties was achieved, but the effectivity of the cult's attacks was undermined by unresolved technical difficulties, and probably also by the vagaries of cult-dominated behavior within the group. Aum Shinrikyo has been the only non-state organization known to potentially develop a weapon of mass destruction (WMD).

Complex toxic chemicals are produced by reacting precursor chemicals together, usually through a series of chemical reactions, each of which requires particular conditions of heating or cooling, the handling of gases, the requirement for catalysts and/or quenchers, and often the use of specialized and/or inert reaction vessels [13, 14]. To obtain high agent purity will also often require special equipment. Some ubiquitous chemical precursors can be ordered in relatively small amounts without undue suspicion, but others may require legitimization by setting up an elaborate front company to reduce the suspicions of suppliers.

Small quantities of chemicals are likely to escape detection [11]. The Chemical Weapons Convention requires reporting of all facilities that use more than 100g of certain military precursors with no commercial use, more than 1 tonne a year of a defined group of high-risk dual-use precursors, and of 30 tonnes per annum usage of lesser-risk precursors in common commercial usage [15]. Since 1985, international export control of such agents has reflected the conventions of the Australia Group of major chemical suppliers. Equipment for the small-scale synthesis of CW in kilogram quantities would probably fall below export thresholds. Indeed, a small production line for several CW agents could be set up on the bench using laboratory glassware [11]. Risks from fires, explosions, and leaks in production and storage at small-scale facilities would be a constant threat.

Skilled mechanical and electrical engineers could build a satisfactory chemical sprayer or explosive burster. Small-scale production is compatible with unconventional dissemination methods, such as from trucks, boats, from crashing into a building, using backpacks, canisters, fire extinguishers, or crop-dusters.

The question is whether terrorists have sufficient motivation and financing to undertake the technical developments necessary for CW success. Direct use of commercially available hazardous chemicals and the purchase of stolen weaponized chemicals are easier options, should opportunity present itself. Among commercially available poisons that could be used as a small-scale weapon are heavy metals; volatile toxins such as benzene, chloroform, and trihalomethanes; pulmonary agents such as vinyl chloride, persistent and non-persistent pesticides; and dioxins, furans, and polychlorinated biphenyls (PCBs). Industrial compounds, e.g., cyanides, nitriles, and corrosive acids and bases, might also be obtainable.

Another option for the terrorist with inadequate technical capabilities is to sabotage or bomb a critical area of an already existing chemical plant. During favorable weather conditions a toxic cloud could be released over an adjacent population area. Knowledge of chemical plants would be a prerequisite. An almost entirely indiscriminate attack might result, but in certain circumstances a dangerous weapon could be created. The most salutary example is the accidental release of methylisocyanate from a Union Carbide insecticide plant in Bhopal, Madhya Pradesh, India, in 1984. Eleven thousand persons were disabled and up to 3,800 individuals died [10]. This accident led to an EPA-enforced Toxics Release Inventory (TRI) for 66,000 industrial facilities across the US that provides enhanced awareness of the presence of hazardous chemicals within the community, and facilitates disaster management planning. The Offsite Consequence Analysis (OCA) part of these reports are not released to the public in case this information might encourage terrorism [16].

Although considerable public comment equates vulnerability to chemical attack on civilian populations with a finite threat, the relationship between the two incorporates many variables, both known and unknown, including the strategic motivation of terrorists [17]. The most feasible chemical attack would in an enclosed space, in a building, indoor stadium, or convention center. With limited CW availability, indoor dissemination might be expected to be more successful than open-air attack. For several reasons, therefore, it is doubtful that a non-statal adversary could target effectively a group of people larger than a few hundred with any kind of chemical attack [18].

Having explored the vulnerability to chemical attack, it is useful to reflect that there was only one fatality from CW attack within the US homeland during the twentieth century. In 1973, the homegrown Symbionese Liberation Army terrorist group assassinated a Californian school superintendent with a cyanide-tipped bullet [19]. Some perspective is needed in assessing the current risk of the US to chemical attack. If it is decided that, indeed, cogent asymmetric threats exist to the US civilian population, the nation must assess the magnitude of the investment necessary to counter that threat. The possibility of a low-probability cata-

strophic event has to be weighed against the possibility of public health hazards of higher probability but of much smaller magnitude. Preparedness can itself be a deterrent.

INDUSTRIAL CHEMICALS AS TERRORIST AGENTS

Industrial production since the late nineteenth century has continued to generate exponential increases in the number of toxic substances identified. Currently as many as 500,000 US commercial products pose physical or health hazards [20]. In 1999, the Environmental Protection Agency (EPA) estimated that approximately 850,000 facilities in the country were working with hazardous chemicals. Indeed, there are perennial risks of releases of hazardous materials (hazmats) because of mishaps in chemical manufacturing and storage, from industrial accidents in other sectors of the economy, as a result of transportation accidents, or from accidents in the home. Most chemical spills are small with few casualties [21]. HAZMAT response guidelines, training, and equipment have been standardized by the National Fire Academy (NFA) and the Federal Emergency Management Agency (FEMA) in order to manage hazardous chemical accidents efficiently [22]. A newly perceived threat to the US homeland involves the deliberate use by terrorists of chemical weapons against civilian populations with the purpose of maximizing casualties. Industrial chemicals are ubiquitous in many counties across the United States and might be utilized in chemical terrorism, particularly perhaps by indigenous terrorists. To assist local public health and safety officials in preventing and mitigating such hazards, the Agency for Toxic Substances and Disease Registry (ATSDR) has proposed a 10-step procedure [23] to formalize local and regional planning.

- Identify, assess, and prioritize threats
- Identify local sources of chemicals with attendant risks
- Evaluate potential exposure pathways
- Identify potential acute and chronic health impacts
- Estimate potential infrastructure and environmental effects
- Identify health risk communication requirements
- Identify methods to mitigate potential hazards
- Identify preventive methods to reduce access to candidate CW
- Incorporate threat assessment, mitigation, and prevention strategies into emergency response plans
- Training exercises to prevent and mitigate identified hazards

The enhanced political accountability that improved awareness of the presence of hazardous chemicals within the community has brought better security in chemical production and storage facilities. Chemical transportation remains a vulnerable area in which future improvements must be made.

One of the major problems in combating chemical terrorism is the presence of dual-use chemicals. Table 21.2 shows several of these dual-use chemicals. As can be seen from this table, a number of chemicals are also the precursor for a number of chemical warfare agents. Also the globalization of the chemical industry has led to large international flows of these dual-use chemicals. For example, chemicals such as ammonia, ethanol, isopropanol, sodium cyanide, yellow phosphorus, sulfur monochloride, hydrogen fluoride, and sulfur are commodity chemicals that are used in commercial industry at the level of millions of tons per year and hence are impossible to control. And these chemicals are precursor chemicals for Tabun agent. Hydrogen fluoride is another chemical necessary for production of G agents. However, it is used at many oil refineries and can be purchased commercially in large quantities; it is also easily derived from phosphate deposits, which usually contain fluorides. Some chemicals, although they can be used to produce chemical agents, may be controlled to some extent because they are manufactured in much smaller volumes. These chemicals include phosphorus trichloride (with 40 producers world-wide), trimethyl phosphite (21 producers), and — for tabun only—phosphorus oxychloride (40 producers). Even then, some chemicals have important use; for example, phosphorus oxychloride is used extensively in commercial products such as hydraulic fluids, insecticides, flame-retardants, plastics, and silicon. Similarly, di-methyl methylphosphonate (DMMP), an intermediate in nerve-agent production, is produced as a flame retardant by 11 companies in the United States and 3 in Europe (Belgium, United Kingdom, and Switzerland).

COUNTERMEASURES

Most of the developing countries cannot establish a chemical factory for production of chemical agents without the help of western countries. They will need assistance in the area of equipment design, installation, and in start-up. A number of equipment generally has to be purchased from western countries. Because of this dependency, Western governments have attempted to slow CW proliferation by establishing a committee known as the Australia Group, which coordinates national export-control regulations to restrict the sale of key CW precursors to suspected proliferants. Nevertheless, the export controls coordinated by the Australia Group cannot prevent countries that are outside this body from selling precursor chemicals. The problem may be with the terrorist groups, which may not have the capability or resources to set up a plant for producing chemical agents, but they can certainly buy them from other countries. Nevertheless, there are a number of indicators that can be monitored for tracking chemical agent proliferation or manufacturing activities by a country.

Doestically a number of dangerous chemicals with the potential to be used either in improvised weapons or as premeditated releases are available. These chemicals have a number of industrial uses but must be registered with ATSDR

soft targets. These include: chemical manufacturing plants (chlorine, peroxides, other industrial gases, petroleum, plastics, and pesticides); food processing and storage facilities (ammonia tanks); water purification plants (chlorine tanks); chemical transportation assets (rail tank cars, tanker trucks, pipelines, river barges); gasoline and jet fuel storage tanks (airports, distribution centers, barge terminals); compressed gases (tanks, pipelines, and pumping stations); gold mines (cyanide and mercury compounds); pesticide manufacturers and distributors (organophosphates); and research and medical laboratories.

Table 21.2 Dual-Use Chemicals

Dual-use chemical	CW agent	Commercial product
Thiodiglycol	Sulfur mustard	Plastics, dyes, inks
Thionyl chloride	Sulfur mustard	Pesticides
Sodium sulfide	Sulfur mustard	Paper
Phosphorus oxychloride	Tabun	Insecticides
Dimethylamine	Tabun	Detergents
Sodium cyanide	Tabun	Dyes, pigments, gold recovery
Dimethyl methylphosphonate	G Agents	Fire retardants
Dimethyl hydrochloride	G Agents	Pharmaceuticals
Potassium bifluoride	G Agents	Ceramics
Diethyl phosphite	G Agents	Paint solvent

Source: Giovanni A. Snidle, "United States Effort in Curbing Chemical Weapons Proliferation," U.S. Arms Control and Disarmament Agency, *Military Expenditures and Arms Transfers 7939* (Washington, DC: U.S. Government Printing Office, October 1990), p. 23 [24].

Considerable hazardous material control infrastructure may be in place at larger industrial facilities. Chemical transportation assets present more difficult hazards as they are more difficult to protect and because large quantities of chemicals can be moved adjacent to potential targets, as illustrated by the April 2002 bombing of the Djerba synagogue in Tunisia using a propane truck. The risks of some common commercial chemicals[23] are shown in Table 2.

Unlike military CW attacks, ingestion may be an important route of exposure in chemical terrorism, particularly with cyanides, heavy metals, and liquid aromatic hydrocarbons, such as benzene. In such complex chemical environments, reference to Regional Poison Centers, to the North American Emergency Response Guidebook (hazmat.dot.gov/gydebook.htm), to commercial databases such as Tomes Plus by Micromedex (www.micromedex.com/products/tomesplus) or Chemtrec (www.cwc-chemical.com/chemtrec.htm) and to data sheets from the

Agency for Toxic Substance and Disease Registry (www.atsdr.cdc.gov/) and the Environmental Protection Agency.

Table 21.2 Potential CW Risks of Common Commercial Chemicals.

Nature of improvised CW	Chemical agents
Eye/skin/respiratory irritant	Acids, ammonia, acrylates, aldehydes, isocyanates
Choking agent	Chlorine, phosgene, hydrogen sulfide
Asphyxiates	Aniline, nitrile, cyanide compounds, vinyl chloride
Nerve agents	Organophosphate pesticides
Blister agents	Dimethyl sulfate
Flammable industrial gases	Acetone, alkenes, alkyl halides, amines
Water supply contaminants	Benzene and other aromatic hydrocarbons
Oxidizers for improvised explosives	Oxygen, butadiene, peroxides
Incendiaries	Natural gas, propane, isobutane, petroleum

One important consequence of the recent concern over the potential misuse of dangerous chemicals within the community is the realization that plant security and security around chemical transportation assets has been poor and that regulatory improvements are urgently required. The identification and security of potential terrorist chemical targets cannot be ignored. The US government-led efforts to enhance hazardous materials preparedness for chemical releases will better prepare communities to respond to chemical terrorism events if or when they occur.

INDICATORS OF CHEMICAL AGENT PROLIFERATION ACTIVITIES

Verification of production of chemical agents is a challenging task. It is not necessary for a facility that produces chemicals to be large. A small production facility could manufacture significant quantities of CW agent over several years. Several potential indicators, or "signatures," of CW development, production, and weaponization may be used to detect chemical agents production intentions of a country or a terrorist group. Each signature taken in isolation is probably inadequate to identify such facility, but a "package" of signatures from various sources may be highly suggestive of a CW capability. Some of these signatures are discussed below. A detailed discussion of these signatures can be found in reference [25].

Research and Development Signatures

A country interested in developing a CW capability may first try to initiate its own laboratory research for development of chemical agents. The country may

involve a core group of their scientists or chemists, although this step is not necessary if standard agents and known production processes are to be employed. However, a terrorist group may try to recruit scientists to set a small laboratory. A prominent scientist generally likes to publish his work in scientific journals. Sudden disappearance of his contribution to the scientific journal may be an indicator that he is engaged in some other activities that do not allow him to publish.

External Production Signatures

Since so much of CW agent production involves dual-use technologies, it is difficult to distinguish between illicit and legitimate production. However a country's certain interest in production of chemicals involving the same precursor chemical that are used for production of chemical agents should be taken seriously and investigated. Aerial photograph and remote sensing may be used to gather external evidence of such activities.

Internal Production Signatures

Under the CWC verification regime, external signatures obtained non-covertly through overhead photography and remote sensing will be supplemented with internal signatures obtained by authorized onsite inspections.

Chemical Signatures

The goal here is to collect and analyze samples during on-site inspections of chemical plants and suspect facilities and to detect signatures of illicit CW production.

Detecting Clandestine Production

Detection of clandestine CW agent production in a non-declared facility would require non-cooperative data collection by human agents or by covertly emplaced or remote sensors, which might then be used to cue a challenge inspection.

COMPONENTS OF A COMPREHENSIVE CHEMICAL WEAPON COUNTERTERRORISM STRATEGY

Treaties on the prohibition of the use of chemical weapons date back to 1946, the latest being the September 3, 1992 treaty and opened for signing on January 13, 1993. One hundred and seventy-four countries have signed the agreement as of February 2001. United States ratified the agreement on April 25, 1997 and Russia in November 1997, and Afghanistan in 1993.

According to the CWC agreement, countries manufacturing toxic chemicals, precursors, and other chemicals noted in Table 17.1 must notify OPCW. As many chemicals in this list are toxic but are used for the manufacture of other useful

chemicals, it is necessary for the parties manufacturing such chemicals to declare plant sites that produce aggregate quantities of discrete organic chemicals (DOC) in excess of 200 tons per year as well as plant sites which include a plant producing more than 30 tons per year of a DOC containing the elements phosphorus, sulfur, or fluorine. Production data for such plant sites must be provided. Routine inspections of the facilities are carried out. In spite of these and other regulations, several chemicals can get into the hands of terrorists or terrorist organizations to manufacture chemical weapons.

However, OPCW is trying to have further control over the production and/or knowledge of the chemicals agents that are produced worldwide and to safeguard them. Table 21.3 is a summary of Reporting and Inspection Requirements under the Chemical Weapons Convention. The amounts of chemicals noted are based on per annum production. Inspections are to begin after three years. Production is calculated over an entire plant site, chemical-by-chemical, except for unscheduled DOCs, for which all unscheduled DOCs produced at a plant site should be aggregated. PSF chemicals should be aggregated plant wise and chemical-by-chemical. Initial reports by ratifying States to the OPCW will be due 30 days after the Convention enters into force. Reports to the OPCW (Organization for the Prohibition of Chemical Weapons) by national Governments will be due annually thereafter, with separate declarations for past and anticipated activities. Governments will also be required to report any additionally planned activities at reporting facilities. The details of national reporting procedures are left to national governments, which may wish to institute their own procedures to ensure compliance. These notes are written to show that in spite of the international controls and inspections in place, terrorists manage to get hold of chemicals for their use.

Asymmetric warfare is being employed by terrorist groups so as to avoid US strengths and to attack covertly its vulnerabilities. International disarmament remains an important component of any counterterrorism strategy under the 1993 Chemical Weapons Convention. Other strategic endeavors are also critically important [26], including counter-proliferation, pre-emption, deterrence, and crisis and consequence preparedness. The chemical weapon disarmament protocols are dependant upon levels of state cooperation that, to date, has proven difficult to achieve [27], although the diplomatic efforts are ongoing. Despite these difficulties, as of early 2002, 15% of the reported worldwide manifest of CW have been destroyed and the process is accelerating according to treaty commitments. US concerns remain as to the verifiability of the CW control monitoring provisions, yet Washington continues to oppose some of the intrusive verification procedures, as they apply to the US.

Counter-proliferation means aggressive action to limit the spread of CW technology, either multilaterally or unilaterally. The miscalculated dependence upon electronic and remote intelligence gathering among US intelligence agencies in the 1990s led to loss of capability in human intelligence [28] which is necessary if well organized and disciplined substate terrorist groups are to be penetrated. Human intelligence provides the best information on the intentions of potential

enemies, may reveal early warnings of potential attacks, and inform as to perpetrators and sponsors. The necessary intelligence redirection will undoubtedly be achieved once the intelligence lessons of the World Trade Center attacks are integrated.

Table 21.3 Summary of reporting and inspection requirements under the CWC (OPCW, 2001).

Chemical	Reporting Threshold	Inspection Threshold	Affected Organizations
Schedule 2 A	100 kg	1 ton	Producers, processors, consumers, importers, and exporters
Schedule 2 A	1 kg	10 kg	Producers, processors, consumers, importers, and exporters
Schedule 2 B	1 ton	10 tons	Producers, processors, consumers, importers, and exporters
Schedule	330 tons	200 tons	Producers, importers, and exporters
Unscheduled	200 tons	200 tons	Producers
Discrete Organic Chemical			
PSF Chemicals	30 tons	200 tons	

Pre-emption involves the disruption of terrorist efforts by dislocating long-term financial and logistic support, impairing command structures, and intervening decisively when preparations for a terrorist attack are detected. Intelligence gathering and analysis underpins these efforts, often in collaboration with international partners. Domestic homeland measures and awareness may also be contributory. Antiterrorist pre-emptive activities merge with the FBI crisis management responsibilities. There are a number of recent publications that can be recommended to help in the understanding of the terrorist enemy [29, 30].

Deterrence requires both the development of a response capability and the political willingness to undertake massive retribution against terrorist attacks. A framework for retribution is indeed incorporated in the 1993 CW Convention. Such an international legal framework has led in recent years to multilateral actions in Iraq, Afghanistan, Libya, Bosnia, and Kosovo. The extraordinary technological superiority of US forces provides a formidable deterrent reality to international terrorism, and which is coupled with the contemporary international political will to wage a war of attrition on terrorists and upon the parastatal structures

that support them. A clearly enunciated policy must be established that host nations, supported by the international community, will act decisively each and every time that their citizens are threatened by terrorist action.

Crisis response preparedness to a CW attack is under the leadership of the FBI, and CW consequence management is organized under the leadership of FEMA. Both build upon the local and State CW incident preparedness of hazardous materials (HAZMAT) crews, fire departments, emergency medical service personnel, and police officers. In recent years, the perceived increased national risk of chemical (and biological) terrorism has led to considerable CW training [31-34], budgetary support, and equipment grants under the National Response Plan (chapter) for all first responders to enhance their response capabilities irrespective of prior experience, and these efforts continue. A well ordered emergency response can modulate considerably the sequelae of CW attacks and contribute to undermining the terrorist goals.

REFERENCES

1. Chemical Casualty Care Division. U.S. Army Medical Research Institute of Chemical Defense. Medical Management of Chemical Casualties Handbook, 3rd edition. Aberdeen Proving Ground, MD, USAMRICD, 2000.
http://ccc.apgea.army.mil/reference_materials/handbooks/RedHandbook/001TitlePage. (April 6, 2002)
 2. Anonymous. Dissemination, dispersion, and weapons testing. In Military Critical Technologies List, Part II: weapons of Mass Destruction Technologies, Section 4, Chemical Weapon Technology. Washington D.C. Office of the Under Secretary of Defense for Acquisition and Technology, 1998. www.fas.org/irp/threat/mct198-2/p2sec04.pdf. (April 6, 2002).
 3. Stockholm International Peace Research Institute. The Problem of Chemical and Biological Warfare. A Study of the Historical, technical, Military, Legal, and Political Aspects of CBW and Possible Disarmament Measures. Vol 2. CB Weapons Today. New York: Humanities Press, 1973.
 4. Organization for the Prohibition of Chemical Weapons (OPCW). Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Geneva, Switzerland, 1994.
 5. WHO Group of Consultants. Health Aspects of Biological and Chemical Weapons: WHO Guidance. 2nd edition. World Health Organization. Geneva, Switzerland, 2002. www.who.int/emc/book_2nd_edition.htm (April 6, 2002).
 6. Organization for the Prohibition of Chemical Weapons (OPCW). Instant Briefing. www.opcw.org/ib/index.html (May 8, 2002).
-

7. B Spring. The chemical weapons convention: a bad deal for America. In *Chemical and Biological Warfare. The Reference Shelf*. B Solomon, Ed. New York: HW Wilson. 71(3): 49-67, 1999.
8. AH Cordesman. Proliferation and Response. Department of Defense. Washington D. C. 2001.
9. AE Smithson. Stay the course on chemical weapons ban. *Issues in Science and Technology*. University of Texas at Dallas. P 37-40, 1998. www.nap.edu/issues/14.2/smiths.htm (May 8, 2002).
10. AH Cordesman. *Defending America: Redefining the Conceptual Borders of Homeland Defense. Terrorism, Asymmetric Warfare and Chemical Weapons*. Center for Strategic and International Studies. Washington D. C. 2001. www.csis.org/homeland/reports/terrorasymw&chem.pdf. (April 6, 2002).
11. RA Falkenrath, RD Newman, BA Thayer. *America's Achilles Heel. Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, MA: MIT Press, 1998.
12. DE Kaplan. Aum Shinrikyo. In: *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Tucker JB, ed. Cambridge, MA: Belfer Center for Scientific and International Affairs, Harvard University, 2000, pp 207-226.
13. Office of Technology Assessment. *Technologies Underlying Weapons of Mass Destruction, OTA-BP-ISC-115*. Washington DC: OTA, 1993. <http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk1/1993/9344/9344.PDF>
14. General Accounting Office. *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks, GAO/NSAID-99-163*. Washington DC: GAO, 1999. Internet: <http://www.gao.gov/archive/1999/ns99163.pdf> Accessed April 6, 2002.
15. AE Smithson, D Mahley, E. Harris. *The Chemical Weapons Convention Handbook, Stimson Center Handbook No.2*. Washington DC: Henry L. Stimson Center, 1995.
16. Environmental Protection Agency. Title 40: Chapter 1, Part 370. Hazardous chemical reporting: community right-to-know. http://www.access.gpo.gov/nara/cfr/cfrhtml_00/Title_40/40cfr370_00.html
17. N Gurr, B Cole. *The New Face of Terrorism. Threats from Weapons of Mass Destruction*. London: Tauris, 2000.
18. R Purver. *Chemical and Biological Terrorism: the Threat According to the Open Literature*. Ottawa, Canadian Security Intelligence Service, 1995. Internet: http://www.csis-scrs.gc.ca/eng/miscdocs/tabintr_e.html Accessed April 6, 2002.
19. JB Tucker, A Sands. An unlikely threat. *Bull Atomic Scientists* 1999;55(4):46-52. Internet: <http://www.thebulletin.org/issues/1999/ja99/ja99tucker.html> Accessed April 6, 2002.

20. National Disaster Education Coalition. Chemical Emergencies. Internet: <http://www.disastercenter.com/guide/chemical.html> Accessed April 6, 2002.
21. S Binder. Deaths, injuries and evacuations from acute hazardous material releases. *Am J Public Health* 1989;79:1042-1044.
22. US Department of Health and Human Services. Managing Hazardous Materials Incidents (MHMI), vol 1, 2, and 3. Atlanta, GA: Agency for Toxic Substances and Disease Registry, 2001. Internet: <http://www.atsdr.cdc.gov/mhmi.html> Accessed April 6, 2002.
23. JL Hughart, MM Bashor. Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention. Atlanta, GA Agency for Toxic Substances and Disease Registry, US Department of Health and Human Services, 1999. Internet: <http://www.techstuff.com/terror/terror.htm> Accessed April 6, 2002.
24. AS Giovanni. "United States Effort in Curbing Chemical Weapons Proliferation," U.S. Arms Control and Disarmament Agency, Military Expenditures and Arms Transfers 7939 (Washington, DC: U.S. Government Printing Office, October 1990), p. 23 [24].
25. Technical Aspects of Chemical Weapon Proliferation. www.fas.org.
26. FJ Cillufo, SL Cardash, GN Lederman. Combating Chemical, Biological, Radiological and Nuclear Terrorism: a Comprehensive Strategy. Washington DC: Center for Strategic and International Studies, 2000. www.csis.org/homeland/reports/combatchembiorad.pdf.
27. JB Tucker. Nonproliferation Regimes at Risk. Challenges to the Chemical Weapons Convention. CNS Occasional Papers:#3. Monterey Institute of International Studies, 2002. Internet: <http://cns.miis.edu/pubs/opapers/op3/tucker.htm> Accessed May 8, 2002.
28. C Quillen. State Sponsored Terrorism: a Growing Threat. Terrorism Research Center, 2002. Internet: <http://www.terrorism.com/analysis/index.shtml> Accessed May 8, 2002.
29. B Hoffman. Inside Terrorism. New York: Columbia University Press. 1998.
30. DJ Whittaker. Ed. The Terrorist Reader. London: Routledge. 2001.
31. Hazardous Materials Emergency Preparedness Grants (HMEP): Response Training Guidelines. United States Fire Service/ Federal Emergency Management Agency, 2002. <http://www.usfa.fema.gov/hazmat/hmep/HMEPResponse.pdf>.
32. United States Fire Administration. Hazardous Materials Guide for First Responders, 2002. Internet: <http://www.usfa.fema.gov/hazmat/>.
33. Agency for Toxic Substance and Disease Registry, US Public Health Service. Managing Hazardous Materials Incidents, Vol 1, Emergency Medical Services. Washington

DC: ATSDR, 1992. Internet: <http://www.atsdr.cdc.gov/mhmi.html#V1> Accessed: May 8, 2002.

34. Office of Hazardous Materials Enforcement, Department of Transportation. National Program of Safety Inspection and Enforcement of the Hazardous Materials Regulations. Internet: hazmat.dot.gov/pubtrain/99.2000.multi.pdf.

22

Personal Protective Equipment

Glenn P. Jirka and Wade Thompson

University of Missouri, Columbia, Missouri

INTRODUCTION

Personal protective equipment (**PPE**) is the clothing and other protective gear that workers wear to protect themselves from the environmental hazards associated with a task or job. The “worker” in the case of terrorism response is most often either a warrior (military troop) or a first responder (fire fighter, emergency medical worker, law enforcement officer). Although these two types of responder have markedly different jobs, they face similar environmental hazards while responding to terrorist or potential terrorist activities. Because these environmental hazards are similar, the technologies most often utilized to protect the responder are also very similar.

SELECTING PERSONAL PROTECTIVE EQUIPMENT

There is a wide array of protective clothing and equipment being marketed to both the military and public sector first responder communities. In order to select the best personal protection for a given task, the users must perform a *risk assessment*. In other words, the user must assess the potential hazards, hazard level, and the probability of being exposed to that hazard. Additionally, the user must have a firm grasp of the *doctrine* by which their organization does business in a hazardous environment. The responder must combine the results of their risk assessment, knowledge of their organizational doctrine, and a basic knowledge of PPE *technologies* in order to select the protective equipment available in the marketplace that is best suited for the task at hand. This chapter will address the basic principles of risk assessment as it relates to selecting PPE, the concept of doctrine

as it relates to WMD PPE selection, and the basic technologies that are available in the marketplace to protect responders.

RISK ASSESSMENT

The use of risk assessment techniques to aid in the selection of PPE is common practice in the manufacturing and environmental response sectors. In fact the U.S. Occupational Health and Safety Administration (OSHA) has codified basic hazard assessment and PPE selection guidance in 29 CFR 1910 (Code of Federal Regulations), Subpart I, Appendix B. One method for performing a PPE risk assessment utilizes the following five-step process.

- **Step 1, Define the Mission/Tasks.** The first step to any assessment is determining the type of mission to be performed while wearing the PPE. The type of mission will subsequently dictate the tasks to be accomplished. A member entering a chemical hazard area to draw an air sample will face different hazards than a member entering the same environment to apprehend suspects who may be armed and protected from the chemical hazard.
- **Step 2, Assess the Hazards.** With the mission and tasks in mind, the next step of the assessment process is to identify the hazards and potential hazards to the greatest extent possible. The obvious **weapons of mass destruction (WMD)** hazards include **biological** agents and toxins, **nuclear** devices and radioactive materials, **incendiary** devices, **chemical** agents, and **explosive** devices (termed “b-nice” hazards). In addition to the b-nice hazards, responders must also concern themselves with slip, trip, and fall hazards; heat and cold temperature conditions; sharp objects; and sources of electromagnetic radiation.
- **Step 3, Determine the Risk.** Once all the tasks and possible hazards have been identified the user should identify the areas or systems of the body vulnerable during the given tasks. In addition to the areas of the body that are vulnerable, the user needs to assess the likelihood that the exposure will occur and the consequence of such an exposure. When estimating the likelihood and consequences of exposure, it is advisable to assign numeric values so that priorities can be identified.

Table 22.1 offers one possible system for assigning numeric values to risk. The system results in risk values from zero to one hundred (0 – 100) with one hundred indicating the greatest risk and zero indicating minimal risk. Such a system can be used to quantify risks from all hazards including chemical, biological, radiological, and physical hazards such as slip, trip, and fall hazards. Numeric values will help a user to determine priorities when selecting PPE. For example, if one possible

exposure is to a chemical that is skin absorptive and extremely toxic (causing possible death) through skin absorption and the likelihood of exposure to that chemical is very unlikely, then the estimated risk value would be 20 (10 x 2). Another chemical may produce minor treatable injuries on contact but exposure is likely to be continuous. In this case, the estimated risk value would be 40 (4 x 10).

Table 22.1 Possible system for assigning numeric value to potential exposures when performing risk assessments

Value	Likelihood of Exposure	Consequence of Exposure
0	Extremely unlikely	No health effect
2	Very unlikely	Temporary health effect
4	Unlikely	Minor/treatable injury
6	Likely	Serious injury
8	Multiple exposure likely	Debilitating injury
10	Continuous exposure likely	Probable death

- **Step 4, Compare Need and Available PPE.** Once likelihood and consequence of exposure (risk value) has been assessed, the responder must compare the risk values, available PPE, and the capabilities of the PPE to protect from the various risks. Although at first glance this may appear a simple exercise, many responders find this an extremely frustrating exercise once they begin the process. Responders quickly realize that the PPE required to protect them from all the identified risks often does not exist.
- **Step 5, Select the Most Appropriate PPE.** With the comparison of need and requisite PPE capabilities in hand, the responder must choose the most appropriate PPE for the mission. In other words the responder needs to select the PPE that minimizes risk. In some instances, the responder may find that the possible benefit associated with a mission does not warrant exposing responders to the residual risk and choose to abort the mission. Alternately, responders may find that they can institute environmental or procedural controls that will minimize risks previously identified and allow for safe use of some of the identified PPE.

DOCTRINE

Each response organization has a set of formal and informal beliefs that compose its organizational doctrine. This compilation of core beliefs dictates what the organization and its leaders view as an acceptable level of risk during a given

mission. The level of acceptable risk will subsequently impact PPE selection for the particular mission or task. As an example, consider a response into an indoor environment in which there has already been a dispersal of a chemical agent. Additionally, assume there is potential for the additional dispersion of mist/droplets in the area.

One possible doctrinal point of view is the *no allowable exposure* view. In other words, when dealing with hazardous chemicals (or any hazard), *no exposure* of a user to the chemical is acceptable. This doctrine is based on the belief that all exposure carries with it risk, and that risk to the responder should be minimized regardless of economic or social factors. It places the welfare of the responder above all other considerations. Organizations that prescribe to this doctrine would need to select PPE that totally protects the user from chemical exposure for the entire duration of the mission in the environment given as an example.

An alternate viewpoint is the *as low as reasonably achievable (ALARA)* view. This doctrinal position holds that users should be protected to levels that are “reasonable” taking economic and social factors into account. This viewpoint includes the belief that *all* exposures carry some risk, and subsequently that as exposure increases so does the likelihood of harm. This doctrine is the guiding principle of radioactive material safety. Protection from radioactive materials is considered optimized when the level of protection needed to further decrease exposure is not achievable without an unreasonable social or economic cost. In our example, this ALARA principle would indicate that exposure should be limited to levels not likely to cause injury or illness where reasonable and while considering social and economic factors. In other words, PPE would be selected that would maintain the exposure over a mission period at or below a permissible level.

An alternate doctrine is that of *conditional exposure*. Those who operate under this doctrine hold that exposure to some identified level of a chemical (or other hazard) is acceptable for a particular benefit. For example, an organization may hold that it is reasonable to risk exposure to levels of a chemical that can cause non-permanent injury in order to gain control of a situation. They may believe that allowing exposure to a chemical at levels that may cause serious injury is acceptable if that exposure is likely to facilitate the rescue of viable victims. At the extreme of the conditional exposure spectrum of beliefs is the belief that exposure to levels of a chemical that will likely cause serious health effects or death may be warranted in order to achieve an identified tactical objective. This view is known as the *acceptable losses* viewpoint. In our example, PPE would be selected that allowed for completion of the mission with less regard for the health and welfare of the responder.

Regardless of the specific doctrine that an organization subscribes to, that doctrine will affect the specific PPE selected by the organization. Therefore, in addition to a risk assessment, the individual responsible for selecting PPE for use in various WMD events must have a thorough understanding of their organization’s doctrine. Finally, the responder must have knowledge of the different technologies available to provide protection from the various hazards.

AVAILABLE TECHNOLOGIES

The hazards faced by the terrorism responder fall into five basic categories: biological agents and toxins; nuclear/radioactive materials; incendiary devices; chemical agents; and explosive devices. Each of these hazards acts on the body in one or more ways to inflict its harm. The role of PPE is to prevent or minimize those interactions. The PPE utilized in WMD response can be generally examined in two broad categories: respiratory protection, and dermal protection. Within each of these broad categories there are a few basic types of technology that provide responders with protection from the wide array of materials and situations they may face.

Respiratory Protection

The respiratory tract is designed to allow for the rapid exchange of material between our circulatory system and the surrounding environment. Unfortunately, the same features that make the system so efficient at supporting our respiration also make it sensitive to many of the environmental hazards responders face in WMD incidents. The moist, sensitive and relatively permeable tissues of the respiratory tract may be easily damaged or allow the permeation of unwanted materials and organisms into the body. In fact, many early chemical warfare agents were designed to target the warrior by inflicting harm via the respiratory tract. Consequently, early PPE was designed to protect the respiratory tract of the warrior and his horse as shown in Figure 22.1.

Respiratory protection equipment currently utilized for WMD response can be classified as either *atmosphere-supplying* or *air-purifying* equipment. The primary difference between the two types of respirator lies in the source of the air the user inhales. In an air-purifying respirator, the air comes from the immediate surroundings of the user. Atmosphere-supplying respirators utilize a controlled air source known to be safe for respiration and free of contaminants.

Air-Purifying Respirators

The *air-purifying respirator*, referred to as an APR, filters and/or chemically scrubs the user's air prior to inhalation. APRs are relatively lightweight, easily transportable, offer relatively long mission durations, and can be effective for specified atmospheres. In order to ensure effectiveness, the APR must be fitted with a cartridge(s) that is appropriate for the atmosphere being entered. For example, HEPA (high efficiency particulate) filters are used to filter particulate matter such as asbestos, radioactive particles, and biological agents such as anthrax spores. Alternately, organic vapor cartridges are utilized for filtering many of the organic-based chemical agents. Figure 22.2 shows a schematic view of a full-face APR.

APR cartridges and filters have several limitations. The functional life of a cartridge is limited and requires it be replaced at designated intervals after opening

the sealed container in which it is packaged. The cartridges and filters also have shelf lives and must be discarded upon expiration to avoid degraded performance.



Figure 22.1 Cavalry soldier and horse each utilizing an air-purifying respirator to protect the respiratory tract.

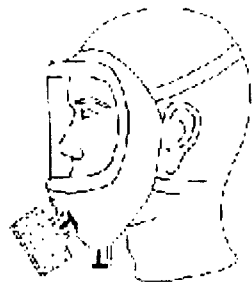


Figure 22.2 Schematic representation of an air-purifying respirator (APR).

Additionally, although cartridges are effective at purifying air passing through them, they do not produce oxygen and therefore cannot be used in oxygen-deficient atmospheres. Finally, the APR user has the added respiratory burden caused by pulling the inhaled air through the cartridges.

In order to reduce the stress placed on the user using an APR, APRs equipped with powered fans have been introduced in the market place. These fan-powered APRs are known as *powered air-purifying respirators* or PAPRs. Figure 22.3 shows a typical PAPR composed of a hooded loose-fitting facepiece that is connected to a fan unit by a breathing hose. The belt mounted fan unit draws air through the filters and forces air through the breathing tube to the facepiece of the respirator. PAPRs are powered by either disposable or rechargeable batteries and typically can operate for approximately six hours before replacement.

Atmosphere-Supplying Respirators

Atmosphere-supplying respirators are those that supply air from a fixed source directly to the user. The atmosphere is typically supplied from a cylinder of pressurized air either carried by the user or maintained within 300 feet. Air is allowed to flow to the user through a pressurized hose from the cylinder. Although not commonly used by responders, the air supply may also be a breathing air compressor located near the use site.



Figure 22.3 A hooded loose-fitting facepiece powered air-purifying respirator . Note the fan/filter unit in the foreground with the battery.

Atmosphere-supplying respirators are viewed as the highest level of respiratory protection available. They provide the highest level of protection because they supply a known-safe air supply to the user. However this characteristic leads

to a number of disadvantages to using this type of device during WMD response. The user must carry their air supply in a cylinder or be tethered to the air supply. Compressed breathing air is carried in metal or composite cylinders on the back or waste of the user. These cylinders are relatively heavy and must be refilled after twenty to sixty minutes of operation in the most commonly used configuration. This configuration of the supplied-atmosphere respirator is known as a self-contained breathing apparatus (SCBA). The SCBA shown in Figure 22.4 is commonly used by responders to WMD events and operates in an open-circuit mode. Open circuit SCBA users exhale their respirations out of the system and to the atmosphere. Closed-circuit SCBA recycle or scrub exhaled air in an attempt to maximize use of the air supply. Closed-circuit SCBA have seen limited use in the WMD arena because they can increase mission duration up to approximately two to four hours but are more bulky than open-circuit SCBA and may hamper operations.



Figure 22.4 Responder wearing a level B ensemble consisting of a self-contained breathing apparatus and a splash-protective non-woven polymer coverall. *Photo courtesy of the University of Missouri Fire and Rescue Training Institute.*

Respirator Design

Respirator designs vary widely and can markedly affect the way a respirator protects a user from a given hazard. Respirators may be either tight fitting or loose fitting. Tight fitting respirators are those that press tightly against the user's face and seal the surrounding atmosphere out. Tight fitting respirators require that users be properly fit and require that nothing pass between the seal of the respirator and the face. This requirement precludes users with facial hair or eye wear that breaks the seal of the mask from utilizing the respirator. Tight fitting respirators are available in either full face or half-face construction. Half-face tight-fitting respirators encapsulate the nose and mouth but leave the eyes exposed. Full-face tight-fitting respirators encapsulate the eyes, nose and mouth and are preferred because they provide additional protection to the eyes which are a primary point of chemical absorption.

Loose fitting respirators are constructed as hoods that enclose the user's head and secure around the upper torso or neck. Air flow into the hood prevents contaminated air from entering the user's air supply. This configuration allows users with facial hair and eyewear to utilize a respirator without altering the eyewear or facial hair. They do however use more air because of the air required to maintain the air flow out of the hood. This added air flow keeps contaminant from entering the hood. Hooded respirators are either supplied-atmosphere or PAPR style respirators.

Construction materials can also be vitally important to the user of a respirator. Construction materials that allow permeation of chemicals to which the respirator will be exposed are unacceptable. There are several different seal materials used in respirator facepieces, some of which are not as resistive to chemical agents as a user would need to offer protection. Additionally, many respirators designed for use in WMD environments are equipped with shrouds to protect the head from contact with harmful chemicals as shown in Figure 22.5. In addition to a Nomex protective hood, the Swat-Pak™ SCBA shown in Figure 22.4 incorporates black materials to reduce visibility of the wearer in tactical situations.

The National Institute of Occupational Safety and Health (NIOSH) has authority for approving all non-military respiratory protective equipment utilized in the United States. NIOSH requires that respirators be approved for use in the intended environment. This approval requires tests that are designed to ensure that the respirator indeed provides the user with protection. Unfortunately, until recently there was no NIOSH program in place to evaluate SCBA for use in chemical warfare agent environments and thus no SCBAs approved for public safety use in these environments. NIOSH, in January 2002, instituted a program to test and certify SCBA for use in these environments.



Figure 22.5 Self-contained breathing apparatus. *Photo courtesy of Boone County (MO) Fire Protection District Hazardous Incident Response Team and Missouri Urban Search and Rescue Task Force One WMD Response Unit.*

DERMAL PROTECTION

Dermal protection from chemicals, biological materials, radioactive materials, thermal hazards, and blast effects is necessary for responders to WMD type incidents. There is no one garment or suit that provides protection from all these hazards simultaneously, thus the responder to terrorist events must choose from garments based on a variety of technologies and designed for a variety of uses. One convenient manner by which to examine these technologies is by the hazard that they are used to protect from.

Chemical Protection

Chemically protective garments utilized for protection during WMD type events are constructed of materials based on either absorptive technologies or on non-woven polymer barrier technologies. Adsorptive technologies are the basis for the battle dress over-garments (BDO) utilized by military agencies in mission oriented protective posture (MOPP), while non-woven polymer fabrics are commonly associated with industrial chemical protective garments.

Chemical protective garments based on adsorptive technology are constructed in a straightforward manner and often referred to as “permeables.” These garments are based on a carbon-based sorbent core that provides the bulk of the chemical protection. The battle dress over-garment core consists of an activated charcoal impregnated foam. In chemically protective under-garments (CPU) used in Joint Services Light Integrated Suit Technology (JSLIST), a polymerically en-

capsulated activated carbon is utilized to provide the sorptive protection from agents. Civilian first responders are also using the CPU type garments for their response to WMD events.

The sorbent core of these garments is surrounded with an outer and inner shell. These shells are made of fabrics designed to promote air permeability and evaporative cooling. This air flow increases user comfort and decreases heat stress. The outer shell (between the sorbent layer and the environment) is designed to limit liquid penetration or redistribute liquid in order to decrease concentration. The inner shell (the fabric between the core and the user) is designed to wick away perspiration and provide a comfortable interface for the user.

Activated charcoal loses its ability to adsorb contaminants as it is exposed to ambient air, moisture, and contaminants. Therefore, garments based on activated charcoal have lifetimes limited to a few days up to a few months. Users of these garments store them in clean or sealed environments. Additionally, the garments are used for only limited time frames once they have been placed into service. In some instances, these sorbent garments may be laundered and reused a limited number of times.

Non-woven polymer-based garments are composed of a polymer support with one or more barrier film layers laminated to the support. The chemical resistance and physical properties of these multi-layer fabrics varies widely depending on the composition of each layer and the number of layers. For example, some polymer films are excellent at resisting corrosive chemicals yet rapidly degrade when exposed to organic solvents.

Non-woven chemically protective clothing is available in a number of different styles with a variety of different construction features. Typically this clothing is broadly defined as either splash-protective or vapor-protective. Vapor protective clothing is designed to fully encapsulate the user and their respiratory protection within a vapor resistant envelope that provides vapor, liquid splash and particulate protection from the hazardous chemicals which pose the risk. Vapor-protective garments resist both vapor and liquid penetration and permeation. Penetration is the process by which chemicals pass through the garment through openings in the garment such as seams, closures, and imperfections in the material. Permeation is the diffusion of a chemical through the molecular structure of the material. Liquid splash-protective garments protect from liquid penetration or permeation and particulate permeation, but provide little or no protection from vapor hazards.

Selecting a liquid splash-protective or vapor-protective garment can be difficult considering the large number of options in the marketplace. Selection needs to be based on the risk assessment performed, organizational doctrine and a knowledge of the performance of the garment or ensemble considered for use. Unfortunately, performance of garments available in the marketplace varies widely. Therefore, responders often turn to consensus standards to assist them in choosing well constructed general purpose chemically resistant clothing. The most

widely utilized consensus documents for chemically protective clothing are those produced by the National Fire Protection Association (NFPA).

Table 22.2 National Fire Protection Association (NFPA) consensus standards that set minimum performance criteria for chemically protective clothing.

NFPA Standard No.	Current Edition	Title
1991	2000	Standard on Vapor-Protective Ensembles for Hazardous Materials Emergencies
1992	2000	Standard on Liquid Splash-Protective Ensembles and Clothing for Hazardous Materials Emergencies
1994	2001	Standard on Protective Ensembles for Chemical/Biological Terrorism Incidents

The NFPA issues a number of standards that define minimum performance requirements for personal protective equipment utilized during emergency response. These personal protective clothing and equipment standards include the three standards listed in Table 22.2 that define minimum levels of performance for chemical and biological protective ensembles and clothing. The NFPA technical committees responsible for these standards have emphasized an ensemble concept that ensures that protection is designed and tested in such a way as to insure protection at the interfaces between components. In other words, for a splash protective ensemble, its performance against liquid splash is defined as an ensemble including gloves, clothing, boots and all the interfaces between the components of the ensemble rather than as individual items that leave the user to guess at proper interfacing techniques and protection levels.

Specifically, NFPA 1994 (2001 ed.) defines minimum performance standards for three classes of ensembles designed to provide protection to responders responding to chemical or biological terrorism incidents

- **Class 1 Ensembles.** Class 1 ensembles are vapor-protective (EPA level A) ensembles similar to NFPA 1991 compliant garments with reduced abrasion and flame resistance characteristics. Class 1 ensembles would likely be used in environments where droplet or particulate exposure is extremely likely and concentrations of agent are high (at or above the immediately dangerous to life and health (IDLH)).
- **Class 2 Ensembles.** Class 2 ensembles are splash-protective (EPA level B/C) garments that provide a minimal level of vapor protection in addition to the splash protection. Concentration of the hazards in the environment that this ensemble is used will be below the IDLH. A hooded coverall with taped sleeves does not meet the performance requirements of this class. A class 2 ensemble will likely include attached gloves and

visor hoods or shrouds to prevent liquid penetration around the neck of the user.

- **Class 3 Ensembles.** Class 3 ensembles are splash-protective garments (level B/C) that provide no vapor protection. They are likely to be used in areas where there is little threat of direct contamination. Such an environment might include securing a perimeter where exposure levels will be below the short-term exposure limit (STEL).

All three classes require penetration and permeation testing against particular levels of “live” chemical warfare agents such as VX, Sarin (GB), Mustard (HD) and Lewisite (L). The challenge level is greater for class 1 ensembles than for the class 2 and class 3 ensembles. All ensembles are additionally required to resist permeation and penetration from representative toxic industrial chemicals (TICS) or as they are alternately known, toxic industrial materials (TIMs). Finally, the ensembles are required to resist penetration by viral agents as well as provide minimum levels of rip and puncture resistance.

Unlike the permeable garments discussed earlier, the non-woven polymer-based clothing does not allow for air flow or evaporative cooling to any great extent. This characteristic increases the heat stress experienced by the user and often limits the duration of missions that may be performed in this type of garment. However, the overall chemical resistance of the non-woven barrier is typically superior to the permeable technologies. Consequently, gloves, boots and respirator facepieces are constructed out of polymeric materials.

Although chemically protective clothing is classed as either splash-protective or vapor-protective, it is not worn without associated respiratory protection. The U.S. Environmental Protection Agency utilizes a four tier system to classify the respiratory protection/chemical protection combinations used by responders. This classification system, summarized in Table 22.3, is based on four levels of protection commonly used in response and normal chemical handling.

Finally, users must carefully consider the construction features of non-woven chemically protective clothing selected. Garments that look very similar in construction may actually differ greatly. For example, consider two garments constructed out of the same non-woven polymer chemically protective material. Although the portion of the garment that is protecting the majority of the body is made of the same material, the visor materials may be different, the glove materials may be different, or the seams may be closed and sealed differently. In this case, the permeation resistance for the main fabric would be identical but the actual ability of the PPE to resist chemical permeation and penetration may be markedly different.

Biological Protection

Protective clothing designed to protect users from biological agents is commonly produced from the same impermeable polymer membrane films utilized for

the non-woven chemical protection described previously. Garments certified resistant to biopenetration are done so in accordance with standardized test procedures such as the American Society for Testing of Materials (ASTM) Standard F 1671. This test utilizes the surrogate biological agent *Phi-X174 Bacteriophage* to assess resistance to biopenetration. In addition to the protective clothing, respiratory protection including atmosphere-supplying respirators and air-purifying respirators are used to protect the respiratory tract of the responder from inhalation of biological agents.

Table 22.3 National Fire Protection Association (NFPA) consensus standards that cover chemically protective clothing.

Level	Skin Protection	Respiratory Protection	Use
A	Vapor-protective Liquid splash-Protective Particulate-Protective	Supplied Atmosphere Respirator	High splash or immersion environments, vapors skin toxic or corrosive
B	Liquid splash-Protective Particulate-Protective	Supplied Atmosphere Respirator	Incidental splash, limited chemical exposure, hazardous vapors not corrosive to skin or skin toxic
C	Liquid splash-Protective Particulate-Protective	Air-purifying Respirator	Incidental splash, limited chemical exposure, vapors below permissible exposure limits
D	Minimum to no Chemical Protection	N/A	No chemical exposure

Radiological Protection

Protective clothing designed to provide protection from radioactive material is generally designed to meet the requirements set forth for chemical particulate matter or liquid splashes. If an ensemble is capable of protecting from these other hazards, it will also provide protection from radioactive particulate. Radioactive protective equipment typically consists of respiratory protection such as an APR or PAPR with high efficiency particulate (HEPA) filtration and a non-woven polymer film splash protective garment. This type of ensemble limits the likelihood of radioactive particulate entering the respiratory tract, digestive tract and provides dermal protection as well. However, radiation in the form of waves, such as *gamma* or *x-ray* will easily penetrate this ensemble.

Thermal Protection

Responders to terrorism incidents may wear thermal protective gear during initial response to the incident. Responders wear this type of gear for one of two reasons, either because the event has resulted in or poses a threat of fire or because they are firefighters and are utilizing the gear to minimize exposure to chemical or biological agents. Thermal protective gear includes the standard firefighter's gear, proximity gear and entry gear. Entry gear is designed to allow users to make brief entries in areas where there will be direct flame contact with the PPE. Proximity gear is designed for working close to large open flame fires such as those caused by aviation fuel released during plane crashes. Structural fire fighting gear is the most commonly utilized thermal protective gear and is utilized by fire fighters to make entry into burning buildings. It is designed to provide limited thermal protection and a moderate level of physical hazard protection.

Thermal protective gear is constructed of an outer shell, a moisture barrier and a thermal protective layer. The outer shells of these garments are made from fabric woven from durable polymers like Nomex and Kevlar. In some instances the outer shell is aluminized in order to increase its ability to reflect heat from the wearer. The vapor barrier limits the ability of superheated vapors to penetrate the garment and the thermal protective layer consists of one or more layers of thermally insulating material.

In addition to providing thermal protection, structural fire fighting gear has been shown to provide some limited protection from chemical agents when utilized with SCBA. The U.S. Army Soldier Biological Chemical Command (SBCCOM) has tested structural fire fighters gear and issued guidelines for the use of such gear in WMD environments. Although not designed for this use, the gear has been shown under some conditions to allow for the entry into a contaminated area for very brief periods of time in order to rescue a victim. It is, however, important to emphasize that structural firefighters gear is not designed to provide this type of protection and users wearing it in certain environments are at danger of serious health effects and possible death if durations or limiting conditions are exceeded.

Blast Protection

The primary concern of EOD/bomb response unit personnel is achieving blast protection. Blast protection is provided by basic ballistic protective fabrics and vest type technologies commonly in use in the law enforcement community. Additionally, responders need to concern themselves with basic chemical, biological, and radioactive protection because of the potential use of improvised explosive devices (IED) containing contaminants. These "dirty bombs" pose a greater risk to the bomb technician than a standard explosive device. The current state of the art protection available to the EOD/bomb response team member for this type of event utilizes chemical protective clothing beneath blast protective clothing. Although the integration of chemical protection with blast protection seems ini-

tially trivial, the ability of a garment to withstand a blast and chemical penetration at the time of a blast is quite a rigorous task. Figure 22.6 shows a blast protective garment specifically designed to accommodate SCBA and chemically protective clothing. Typically a non-woven polymer garment will be utilized under this garment to provide chemical protection.



Figure 22.6 A bomb technician wearing a SRS-5 blast resistant garment with SCBA and chemically protective undergarment. *Photo courtesy of Missouri State Highway Patrol Bomb Squad.*

EMERGING TECHNOLOGIES

There are ongoing efforts to develop better protective materials and garments for responders to WMD incidents. Many of the efforts utilize technologies currently being utilized in either the high tech or military sector. In some instances these technologies are being simultaneously developed for use in all sectors. For example, selectively permeable membrane materials like those shown in Figure 22.7 are currently under investigation by both private and public agencies. The technology is currently being utilized by the military under a Joint Service Defense Technology Objective. Under this program a selectively permeable membrane is being used to replace the carbon-based sorptive materials normal used in

sorptive garments. Replacing the carbon-based materials with a selectively permeable membrane reduces the garment weight by as much as 50% while maintaining chemical resistance and air flow through the garment. Currently researchers are focusing efforts on a cellulose based membrane and an amine-based membrane.

In addition to the development of improved fabrics, many organizations are working to increase work/mission durations of the user by increasing comfort and

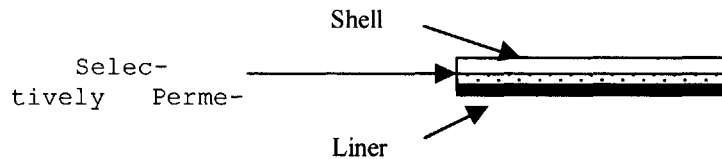


Figure 22.7 Construction schematic of selectively permeable membrane fabrics currently being developed for WMD use.

limiting physiological stress to the user of the WMD PPE. Lightweight microclimate conditioning systems designed to regulate the users physiologic environment and increase work times are being tested by the military. Breathing apparatus designed to regulate the temperature of inhaled air and subsequently provide additional physiological control and comfort are also under investigation in both the public and private sectors.

CONCLUSIONS

Protective clothing utilized by both civilian and military responders to terrorist or WMD type events is diverse and based upon a limited number of technologies. Responders need to have a clear understanding of the risks they face, hazard and risk assessment techniques, their organizational doctrine and the available technologies in order to select appropriate PPE for use at WMD incidents. PPE for use at terrorism incidents is currently evolving in order to provide greater protection to the user, greater comfort and decreased physiological stress on the user.

REFERENCES

1. NJ Bollinger, RH Schultz, NIOSH Guide to Industrial Respiratory Protection, U.S. Health and Human Services, Public Health Service Centers for Disease Control National Institutes for Occupational Safety and Health, Division of Safety Research, September, 1987.
2. J Dunbar, JP Zeigler, "Change of Clothing," Fire Chief, pp30 – 32, July, 2000.

3. GP Jirka, "WMD Protective Clothing for the First Responder," *Advanced Rescue Technology*, August/September, 2001.
4. R Masadi, "*Dismounted Warrior Lightweight-Low Power Microclimate Cooling*," presentation at U.S. Army Soldier Biological Chemical Command Fire and Emergency Services Technology Innovation Conference, March 2001.
5. OSHA 29 CFR 1910 Subpart I, Appendix B.
6. Q Truong, E Wilusz, "*Advanced Lightweight CB Protection*," presentation at U.S. Army Soldier Biological Chemical Command Fire and Emergency Services Technology Innovation Conference, March 2001.
7. JP Zeigler, "FAQs & Fables about Protective Clothing," *Occupational Health and Safety*, pp 42-54, July, 2000.
8. M Ziskin, D Han, D., "*Personal Protective Clothing*," *Hazardous Materials Desk Reference*, Chapter 9, p. 119, New York, NY, McGraw Hill, 2000.

23

The National Response Plan

Julie A. Bentz

*Nuclear Medical Science Officer, National Guard Bureau, Civil Support Office,
Washington D.C.*

INTRODUCTION

Most disasters and emergencies are handled by local and state responders. The federal government is called upon to provide supplemental assistance when the consequences of a disaster exceed local and state capabilities. If needed, the federal government can mobilize an array of resources to support state and local efforts. Various emergency teams, support personnel, specialized equipment, operating facilities, assistance programs, and access to private-sector resources constitute the overall federal disaster operations system. The Federal Response Plan (FRP) describes the major components of the system, as well as the structure for coordinating federal response and recovery actions necessary to address state-identified requirements and priorities.

The FRP employs a multiagency operational structure that uses the principles of the Incident Command System (ICS), based on a model adopted by the fire and rescue community. The system is becoming more standardized in all civilian emergency operations. The International Association of Chiefs of Police has endorsed the system and the National Fire Academy has adopted ICS as the standard for incident response. All incidents will have an Incident Commander (IC) who is responsible for on-scene management. The IC is normally the most senior qualified individual on scene from the local organization with the preponderance of the response assets (typically the local fire or police chief). The IC makes specific requests for assistance through the emergency management system if he or she does not have the assets required for the response. The IC remains in control of the response even when state and federal assets are employed. The ICS will be integrated into a Unified Command System as state and federal assets become in-

creasingly integrated. The ultimate goal of the ICS is to reduce confusion, improve safety, organize and coordinate actions, and facilitate effective management of the incident. ICS can be used in any size or type of disaster to control response personnel, facilities, and equipment. ICS principles include use of common terminology, modular organization, integrated communications, unified command structure, action planning, manageable span-of-control, pre-designated facilities, and comprehensive resource management. The basic functional modules of ICS (e.g., command, operations, logistics, planning, and finance/administration) can be expanded or contracted to meet requirements as an event progresses. Consistent with ICS principles, the FRP can be partially or fully implemented, in anticipation of a significant event or in response to an actual event. Selective implementation through the activation of one or more of the system's components allows maximum flexibility in meeting the unique operational requirements of the situation and interacting with differing state systems and capabilities.

ORGANIZATION OF THE NATIONAL RESPONSE

In the United States, the national Chemical Biological Radiological Nuclear and high energy Explosives (CBRNE) response and subsequent Consequence Management (CoM) operations are conducted by both civil and military response units in a three tier approach. All levels of response may be present in a pre-staged capacity for special event or preplanned activities, or arrive in sequence for no notice events.

1. **First Tier Forces or Local Response.** For no notice response, fire and rescue, law enforcement, or emergency medical service constitute the first tier response consisting of local/multi jurisdictional civil forces operating under the Incident Command System. Existing protocols normally establish the local fire chief as the incident commander. Fire departments evacuate affected areas and initiate operational decontamination using organic equipment. Fire fighters operate in contaminated areas using the self contained breathing apparatus (SCBA). Fire department HAZMAT teams are capable of providing downwind hazard predictions and operation for extended periods in contaminated areas. HAZMAT teams in metropolitan areas are rapidly developing the capability of identifying military chemical agents. Emergency medical personnel will assist in triage and evacuation of victims. The police chief may be the Incident Commander. Local police will prevent additional people from entering the affected areas, enforce evacuation as the Incident Commander deems necessary and secure the incident site.

2. **The Second Tier Forces or State Response.** If the extent of the event exceeds that ability for the first or local tier to manage the consequences of the situation, then state/regional civil and military forces may be activated and deployed in support of the Incident Commander. At this level civil forces include state hazardous materials teams, state police units, and state health department assets, with the national guard providing the state military support. The governor appoints a state

coordinating officer (SCO) to oversee disaster operations of the state. In 22 states and 1 territory, the SCO is the adjutant general. The following agencies will be found in the states, commonwealths and the District of Columbia.

- State Department of Police
- State Emergency Management Office
- State National Guard
- State Office of Energy
- State Department of Environmental Quality (DEQ)
- State Department of Human Services
- Other State Agencies (Department of Transportation, State Health Laboratories, Department of Agriculture, etc.)

3. Third Tier Forces or Federal Response. If the governor determines that the forces and resources available in the state require additional support then the governor requests assistance from the president of the United States. Upon publication of a Presidential Declaration, the federal response plan provides federal asset employment to support the incident commander and governor in managing the consequences of the event. Federal response forces include the Department of Energy's Radiological Assistance Program (RAP) teams, FEMA emergency response assets, the national medical response system, with the Commander in Chief (CINC) Joint Task Force-Consequence Management (JTF-CM) bringing forward federal military support. A federal coordinating officer (FCO) is appointed and is responsible for the timely delivery of federal disaster assistance to the affected state.

FEDERAL DISASTER RESPONSE FRAMEWORK

Each individual federal agency has been designated to provide specific, non redundant support to a disaster scene. Three primary mechanisms for responding to terrorist attacks are based on previously established plans to direct federal support to declared disaster areas. The first of these is the Stafford Act, whose principal purpose is to better coordinate federal disaster relief efforts. The law outlines what constitutes a major disaster and lists the federal aid programs available through the Federal Emergency Management Agency (FEMA) to help alleviate the effects at the local level. The Stafford Act was designed to assist the efforts of the affected states in expediting the rendering of aid, assistance, and emergency services, and the reconstruction and rehabilitation of devastated areas. The Stafford Act defined the scope of existing disaster relief programs by providing an orderly and continuing means of assistance by the federal government to state and local governments in carrying out their responsibilities to alleviate the suffering and damage which result from disasters. It required the development of comprehensive disaster preparedness and assistance plans, programs, capabilities, and organizations by the states and by local governments. Since this law was enacted, there has been a greater coordination and responsiveness of disaster preparedness

and relief programs. The Act provided federal assistance programs for both public and private losses sustained in disasters. The second pillar of the civilian disaster response architecture is the Federal Response Plan that was created in 1992. This plan sets forth fundamental planning assumptions, operational concepts, and specific disaster response duties under the Stafford Act. Altogether, this plan coordinates the efforts of twenty-seven federal agencies with roles in disaster response, as well as the American Red Cross. The Federal Response Plan delineates twelve separate emergency support functions, ranging from transportation to health and medical services, each with a primary federal agency in charge and a number of agencies in supporting roles. The idea behind the Federal Response Plan is to coordinate and leverage existing federal capabilities under FEMA's management. The plan takes an "all hazards" approach toward responding to any type of natural or man-made disaster causing destruction on a massive scale. The third mechanism is the National Disaster Medical System (NDMS). The NDMS is a voluntary network of some seven thousand private citizens and two thousand non-federal hospitals. A public and private sector partnership managed by four federal agencies, the NDMS was created to handle the medical fallout of a catastrophic domestic disaster or a major conflict overseas. The critical functions of the NDMS are to provide rapid medical response, evacuation, and definitive hospital care. The NDMS functions as a back-up to local personnel, providing medical assistance should patient loads overwhelm local and state capacity. Hospitals in over one hundred metropolitan areas participate and pledge to make available collectively more than 110,000 beds. In addition, as a key part of the NDMS, individuals with varying medical backgrounds—including physicians, nurses, and emergency medical technicians—volunteer to form Disaster Medical Assistance Teams in communities across the United States. These teams triage patients at disaster sites and administer immediate medical care to victims. On paper, each team is staffed by anywhere from seventy to one hundred people, although turnout varies from team to team and event to event. The teams are community-based, yet because they can be deployed to other states in times of disaster, they are considered national assets. Once activated, team members become federal employees. Along with the Disaster Medical Assistance Teams, the NDMS also fields a number of specialty teams to handle pediatrics, burns, mortuary affairs, urban search and rescue, mental health, and veterinary services.

EMERGENCY SUPPORT FUNCTION (ESF)

The FRP employs a functional approach that groups under 12 Emergency Support Functions (ESFs) the types of direct federal assistance that a state is most likely to need (e.g., mass care, health and medical services), as well as the kinds of federal operations support necessary to sustain federal response actions (e.g., transportation, communications). In many cases, the state emergency management agency utilizes the FRP's ESFs, modified to adapt to the conditions and opera-

tional environment found in the state. The civil authority designates the affected local as a disaster area, adhering with the state emergency response plans and boundaries adjusted to meet the expanse and conditions presented by the event. In many states, the state emergency management agency has sub-divided the state into regions for emergency management. ESFs are expected to support one another in carrying out their respective missions. Each ESF is headed by a primary agency designated on the basis of its authorities, resources, and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESFs based on their resources and capabilities to support the functional area(s). federal response assistance required under the FRP is provided using some or all of the ESFs as necessary. FEMA will issue a mission assignment to task a primary agency for necessary work to be performed on a reimbursable basis. The primary agency may in turn task support agencies if needed. Specific ESF missions, organizational relationships, response actions, and primary and support agency responsibilities are described in the ESF annexes to the FRP. In cases where required assistance is outside the scope of an ESF, FEMA may directly task any federal agency to bring its resources to bear in the disaster operation. Requests for assistance from local jurisdictions are channeled to the SCO through the designated state agencies in accordance with the state emergency operations plan and then to the FCO or designee for consideration. Based on state-identified response requirements and FCO or designee approval, ESFs coordinate with their counterpart state agencies or, if directed, with local agencies to provide the assistance required. federal fire, rescue, and emergency medical responders arriving on scene are integrated into the local ICS structure.

Emergency Support Function (ESF) #1 — Transportation assists all three tiers of response efforts requiring transportation capacity to perform response missions following a major disaster or emergency. ESF #1 also serves as a coordination point between response operations and restoration of the transportation infrastructure. The primary agency is the Department of Transportation.

Emergency Support Function (ESF) #2 — Communications coordinates federal actions to be taken to provide the required national security and emergency preparedness (NS/EP) telecommunications support to federal, state, and local disaster response elements. This ESF will coordinate the establishment of required temporary NS/EP telecommunications and the restoration of permanent telecommunications. Where appropriate, services may be furnished under provisions of the Telecommunications Service Priority (TSP) system. ESF #2 applies to all federal departments and agencies that may require telecommunications services or whose telecommunications assets may be employed during a disaster response. The primary agency is the National Communications System.

Emergency Support Function (ESF) #3 — Public works and engineering provides technical advice and evaluation, engineering services, contracting for construction management and inspection, contracting for the emergency repair of water and wastewater treatment facilities, potable water and ice, emergency power, and real estate support to assist the state(s) in meeting goals related to life-

saving and life-sustaining actions, damage mitigation, and recovery activities following a major disaster or emergency. The primary agency is the Department of Defense, Army Corps of Engineers.

Emergency Support Function (ESF) #4 — Firefighting detects and suppresses wildland, rural, and urban fires resulting from, or occurring coincidentally with, a major disaster or emergency requiring federal response assistance. ESF #4 manages and coordinates firefighting activities, including the detection and suppression of fires on federal lands, and provides personnel, equipment, and supplies in support of state and local agencies involved in rural and urban firefighting operations. The primary agency is the Department of Agriculture, Forest Service.

Emergency Support Function (ESF) #5 — Information and planning collects, analyzes, processes, and disseminates information about a potential or actual disaster or emergency to facilitate the overall activities of the federal government in providing assistance to one or more affected states. Fulfilling this mission supports planning and decision making at both the field/regional operations and headquarters levels. During disaster operations, ESF #5 becomes the Information and Planning Section of the Regional Operations Center (ROC) or the Emergency Response Team (ERT) at the Disaster Field Office (DFO), as well as the Emergency Support Team (EST) at Federal Emergency Management Agency (FEMA) Headquarters. The primary agency is the FEMA.

Emergency Support Function (ESF) #6 — Mass care coordinates federal assistance in support of state and local efforts to meet the mass care needs of victims of a disaster. This federal assistance will support the delivery of mass care services of shelter, feeding, and emergency first aid to disaster victims; the establishment of systems to provide bulk distribution of emergency relief supplies to disaster victims; and the collection of information to operate a Disaster Welfare Information (DWI) system for the purpose of reporting victim status and assisting in family reunification. The primary agency is the American Red Cross. ESF #6 encompasses emergency shelter for disaster victims and feeding for disaster victims and emergency workers. Emergency first aid will be provided as supplemental to emergency health and medical services. Disaster Welfare Information will be collected and provided to immediate family members outside the affected area through a DWI system. DWI will also be provided to aid in reunification of family members within the affected area who were separated at the time of the disaster. Sites will be established within the affected area for bulk distribution of emergency relief items to meet urgent needs of disaster victims.

Emergency Support Function (ESF) #7 — Resource support provides operational assistance including emergency relief supplies, space, office equipment, office supplies, telecommunications, contracting services, transportation services, security services, federal law enforcement liaison, and personnel required to support immediate response activities. ESF #7 provides support for requirements not specifically identified in the other ESFs. It addresses the effort and activity necessary to evaluate, locate, procure, and provide essential material resources, including excess and surplus property. ESF #7 support may continue until the disposition

of excess and surplus property, if any, is completed. The primary agency is the General Services Administration.

Emergency Support Function (ESF) #8 — Health and medical services provides coordinated federal assistance to supplement state and local resources in response to public health and medical care needs following a major disaster or emergency, or during a developing potential medical situation. Resources will be furnished when state and local resources are overwhelmed and public health and/or medical assistance is requested from the federal government. The primary agency is the Department of Health and Human Services (DHHS). Included in ESF #8 are overall public health response; triage, treatment, and transportation of victims of the disaster; and evacuation of patients out of the disaster area, as needed, into a network of Military Services, Veterans Affairs, and pre-enrolled non-federal hospitals located in the major metropolitan areas of the United States. ESF #8 involves supplemental assistance to state and local governments in identifying and meeting the health and medical needs of victims of a major disaster, emergency, or terrorist attack. This support is categorized in the following functional areas (a) Assessment of health/medical needs; (b) Health surveillance; (c) Medical care personnel; (d) Health/medical equipment and supplies; (e) Patient evacuation; (f) In-hospital care; (g) Food/drug/medical device safety; (h) Worker health/safety; (i) Radiological/chemical/biological hazards consultation; (j) Mental health care; (k) Public health information; (l) Vector control; (m) Potable water/wastewater and solid waste disposal; (n) Victim identification/mortuary services; and (o) Veterinary services.

Emergency Support Function (ESF) #9 — Urban search and rescue rapidly deploys components of the National Urban Search and Rescue (US&R) Response System to provide specialized lifesaving assistance to state and local authorities in the event of a major disaster or emergency. US&R operational activities include locating, extricating, and providing on-site medical treatment to victims trapped in collapsed structures. The primary agency is FEMA.

Emergency Support Function (ESF) #10 — Hazardous materials provides federal support to state and local governments for a coordinated response to actual or potential discharges and/or releases of hazardous materials following a major disaster or emergency. The ESF includes the appropriate response actions to prevent, minimize, or mitigate a threat to public health, welfare, or the environment caused by actual or potential hazardous materials incidents. EPA will carry out the overall management of preparedness and response coordination activities for this ESF.

Emergency Support Function (ESF) #11 — Food identifies, secures, and arranges for the transportation of food assistance to affected areas following a major disaster or emergency or other event requiring federal response. To accomplish this function, activities will be undertaken to identify food assistance needs in the aftermath of a major disaster or emergency. These activities will include coordinating with state, local, and voluntary organizations to determine food assistance needs; obtaining appropriate food supplies; arranging for transportation of those

food supplies to designated staging areas within the disaster area; and authorizing disaster food stamp assistance. The primary agency is the Department of Agriculture.

Emergency Support Function (ESF) #12 — Energy helps restore the Nation's energy systems following a major disaster, emergency, or other significant event requiring federal response assistance. ESF #12 gathers, assesses, and shares information on energy system damage and estimations on the impact of energy system outages within affected areas. Additionally, this ESF works closely with and aids in meeting requests for assistance from state and local energy officials, energy suppliers, and deliverers. Within the ESF #12 agencies are a variety of assets and resources that may be used in response to any event involving energy or multihazard problems. "Energy" includes producing, refining, transporting, generating, transmitting, conserving, building, and maintaining energy systems and system components; "multihazard" includes radiological materials, weapons of mass destruction, and terrorism incidents. Damage to an energy system in one geographic region may affect energy supplies in other regions that rely on the same delivery systems. Consequently, energy supply and transportation problems can be intrastate, interstate, and international. The primary agency is the Department of Energy.

The federal agency designated as an ESF primary agency serves as a federal executive agent under the FCO to accomplish the ESF mission. When an ESF is activated in response to a disaster, the primary agency for the ESF has operational responsibility for orchestrating the federal agency support within the functional area for an affected state; providing an appropriate level of staffing for operations at FEMA Headquarters, the ROC, DFO, and DRC; activating and subtasking support agencies; managing mission assignments and coordinating tasks with support agencies, as well as appropriate state agencies; supporting and keeping other ESFs and organizational elements informed of ESF operational priorities and activities; executing contracts and procuring goods and services as needed; ensuring financial and property accountability for ESF activities; and supporting planning for short and long term disaster operations. When an ESF is activated in response to a disaster, each support agency for the ESF has operational responsibility for supporting the ESF primary agency when requested by conducting operations using its authorities, cognizant expertise, capabilities, or resources; supporting the primary agency mission assignments; providing status and resource information to the primary agency; following established financial and property accountability procedures; and supporting planning for short- and long-term disaster operations. In recovery operations, each federal agency has responsibility for: supporting the FCO in identifying needs and addressing recovery and mitigation program implementation; executing agency programs in an interagency, intergovernmental partnership environment; obtaining funding from the agency's own statutory sources; providing the appropriate level of program staffing to meet common customer service goals and to represent the agency on the ERT; providing status information to the FCO and SCO; and supporting planning for short- and long-term disaster

recovery and mitigation operations. Other federal agencies not signatories to the FRP may have authorities, expertise, capabilities, or resources that may be required to support disaster operations. Those agencies may be requested to participate in federal planning and operations activities, designate staff to serve as representatives to the CDRG, and/or provide support to the field.

PRESIDENTIAL DECISION DIRECTIVE 39 (PDD-39)

Presidential Decision Directive 39 (PDD-39), U.S. Policy on Counterterrorism, establishes policy to reduce the Nation's vulnerability to terrorism, deter and respond to terrorism, and strengthen capabilities to detect, prevent, defeat, and manage the consequences of terrorist use of weapons of mass destruction (WMD). PDD-39 states that the United States will have the ability to respond rapidly and decisively to terrorism directed against Americans wherever it occurs, arrest or defeat the perpetrators using all appropriate instruments against the sponsoring organizations and governments, and provide recovery relief to victims, as permitted by law. Responding to terrorism involves instruments that provide crisis management and consequence management. "Crisis management" refers to measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The federal government exercises primary authority to prevent, preempt, and terminate threats or acts of terrorism and to apprehend and prosecute the perpetrators; state and local governments provide assistance as required. Crisis management is predominantly a law enforcement response. "Consequence management" refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. state and local governments exercise primary authority to respond to the consequences of terrorism; the federal government provides assistance as required. Consequence management is generally a multifunction response coordinated by emergency management. Based on the situation, a federal crisis management response may be supported by technical operations, and by federal consequence management, which may operate concurrently. "Technical operations" include actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed to explosive ordnance or WMD.

The Department of Justice is designated as the lead agency for threats or acts of terrorism within U.S. territory. The Department of Justice assigns lead responsibility for operational response to the Federal Bureau of Investigation (FBI). Within that role, the FBI operates as the on-scene manager for the federal government. It is FBI policy that crisis management will involve only those federal agencies requested by the FBI to provide expert guidance and/or assistance, as described in the PDD-39 Domestic Deployment Guidelines (classified) and the FBI WMD Incident Contingency Plan.

The Federal Emergency Management Agency (FEMA) is designated as the lead agency for consequence management within U.S. territory. FEMA retains authority and responsibility to act as the lead agency for consequence management throughout the federal response. It is FEMA policy to use the Federal Response Plan structures to coordinate all federal assistance to state and local governments for consequence management. To ensure that there is one overall Lead Federal Agency (LFA), PDD-39 directs FEMA to support the Department of Justice (as delegated to the FBI) until the Attorney General transfers the overall LFA role to FEMA. FEMA supports the overall LFA as permitted by law.

Response by agencies to lifesaving and life-protecting requirements under the FRP has precedence over other federal response activities, except where national security implications are determined to be of a higher priority.

CRISIS MANAGEMENT

Unlike disasters of the past, crisis management will play the lead in the overall federal response to threats or acts of terrorism that take place within U.S. territory or in international waters. The Department of Justice (as delegated to the FBI) will be the one overall Lead Federal Agency with FEMA support. The FBI notifies FEMA and other federal agencies providing direct support to the FBI of a credible threat of terrorism. The FBI initiates a threat assessment process that involves close coordination with federal agencies with technical expertise, in order to determine the viability of the threat from a technical as well as tactical and behavioral standpoints. The law enforcement authorities within the affected state are initially notified of a terrorist threat or occurrence by the FBI. If warranted, the FBI implements an FBI response and simultaneously advises the Attorney General, who notifies the President and NSC groups as warranted, that a federal crisis management response is required. If authorized, the FBI activates multiagency crisis management structures at FBI Headquarters, the responsible FBI Field Office, and the incident scene. federal agencies requested by the FBI, including FEMA, will deploy a representative(s) to the FBI Headquarters Strategic Information and Operations Center (SIOC) and take other actions as necessary and appropriate to support crisis management.

If the threat involves WMD, the FBI Director may recommend to the Attorney General to deploy a Domestic Emergency Support Team (DEST). The mission of the DEST is to provide expert advice and assistance to the FBI On-Scene Commander (OSC) related to the capabilities of the DEST agencies and to coordinate follow-on response assets. When a Joint Operations Center (JOC) is formed, DEST components merge into the JOC structure as appropriate. During crisis management, the FBI coordinates closely with local law enforcement authorities to provide a successful law enforcement resolution to the incident. The FBI also coordinates with other federal authorities, including FEMA. The FBI Field Office responsible for the incident site modifies its Command Post to function as a JOC

and establishes a Joint Information Center (JIC). The JOC structure includes the following standard groups: Command, Operations, Support, and Consequence Management. Representation within the JOC includes some federal, state, and local agencies. The JOC Command Group plays an important role in ensuring coordination of federal crisis management and consequence management actions. Issues arising from the response that affect multiple agency authorities and responsibilities will be addressed by the FBI OSC and the other members of the JOC Command Group, who are all working in consultation with other local, state, and federal representatives. While the FBI OSC retains authority to make federal crisis management decisions at all times, operational decisions are made cooperatively to the greatest extent possible. The FBI OSC and the Senior FEMA Official at the JOC will provide, or obtain from higher authority, an immediate resolution of conflicts in priorities for allocation of critical federal resources (such as airlift or technical operations assets) between the crisis management and the consequence management response.

A FEMA representative coordinates the actions of the JOC Consequence Management Group, expedites activation of a federal consequence management response should it become necessary, and works with an FBI representative who serves as the liaison between the Consequence Management Group and the FBI OSC. The JOC Consequence Management Group monitors the crisis management response in order to advise on decisions that may have implications for consequence management, and to provide continuity should a federal consequence management response become necessary. Coordination will also be achieved through the exchange of operational reports on the incident. Because reports prepared by the FBI are "law enforcement sensitive," FEMA representatives with access to the reports will review them, according to standard procedure, in order to identify and forward information to Emergency Support Function (ESF) #5 — Information and Planning that may affect operational priorities and action plans for consequence management.

CONSEQUENCE MANAGEMENT

If there is a credible threat of terrorism, FEMA receives initial notification from the FBI. Based on the circumstances, FEMA Headquarters and the responsible FEMA region(s) may implement a standard procedure to alert involved FEMA officials and federal agencies supporting consequence management. FEMA deploys representatives with the DEST and deploys additional staff for the JOC, as required, in order to provide support to the FBI regarding consequence management. FEMA determines the appropriate agencies to staff the JOC Consequence Management Group and advises the FBI. With FBI concurrence, FEMA notifies consequence management agencies to request that they deploy representatives to the JOC. Representatives may be requested for the JOC Command Group, the JOC Consequence Management Group, and the JIC.

When warranted, FEMA will consult immediately with the Governor's office and the White House in order to determine if federal assistance is required and if FEMA is permitted to use authorities of the Robert T. Stafford Disaster Relief and Emergency Assistance Act to mission-assign federal consequence management agencies to pre-deploy assets to lessen or avert the threat of a catastrophe. These actions will involve appropriate notification and coordination with the FBI, as the overall LFA.

FEMA Headquarters may activate an Emergency Support Team (EST) and may convene an executive-level meeting of the Catastrophic Disaster Response Group (CDRG). When FEMA activates the EST, FEMA will request FBI Headquarters to provide liaison. The responsible FEMA region(s) may activate a Regional Operations Center (ROC) and deploy a representative(s) to the affected state(s). When the responsible FEMA region(s) activates a ROC, the region(s) will notify the responsible FBI Field Office(s) to request a liaison.

If an incident involves a transition from joint (crisis/consequence) response to a threat of terrorism to joint response to an act of terrorism, then consequence management agencies providing advice and assistance at the JOC pre-release will reduce their presence at the JOC post-release as necessary to fulfill their consequence management responsibilities. The Senior FEMA Official and staff will remain at the JOC until the FBI and FEMA agree that liaison is no longer required. If an incident occurs without warning that produces major consequences and appears to be caused by an act of terrorism, then FEMA and the FBI will initiate consequence management and crisis management actions concurrently. FEMA will consult immediately with the Governor's office and the White House to determine if federal assistance is required and if FEMA is permitted to use the authorities of the Stafford Act to mission-assign federal agencies to support a consequence management response. If the President directs FEMA to implement a federal consequence management response, then FEMA will support the FBI as required and will lead a concurrent federal consequence management response.

The overall LFA (either the FBI or FEMA when the Attorney General transfers the overall LFA role to FEMA) will establish a Joint Information Center in the field, under the operational control of the overall LFA's Public Information Officer, as the focal point for the coordination and provision of information to the public and media concerning the federal response to the emergency. Throughout the response, agencies will continue to coordinate incident-related information through the JIC. FEMA and the FBI will ensure that appropriate spokespersons provide information concerning the crisis management and consequence management responses. Before a JIC is activated, public affairs offices of responding federal agencies will coordinate the release of information through the FBI SIOC.

During the consequence management response, the FBI provides liaison to either the ROC Director or the Federal Coordinating Officer (FCO) in the field, and a liaison to the EST Director at FEMA Headquarters. The FCO is responsible for coordinating the timely delivery of federal disaster assistance to the affected state, local governments, and disaster victims. In many cases, the FCO also serves

as the Disaster Recovery Manager (DRM) to administer the financial aspects of assistance authorized under the Stafford Act. The FCO works closely with the State Coordinating Officer (SCO), appointed by the Governor to oversee disaster operations for the state, and the Governor's Authorized Representative (GAR), empowered by the Governor to execute all necessary documents for disaster assistance on behalf of the state. While the ROC Director or FCO retains authority to make federal consequence management decisions at all times, operational decisions are made cooperatively to the greatest extent possible. As described previously, resolution of conflicts between the crisis management and consequence management responses will be provided by the Senior FEMA Official and the FBI OSC at the JOC or, as necessary, will be obtained from higher authority. Operational reports will continue to be exchanged. The FBI liaisons will remain at the EST and the ROC or DFO until FEMA and the FBI agree that a liaison is no longer required.

If an act of terrorism does not occur, the consequence management response disengages when the FEMA Director, in consultation with the FBI Director, directs FEMA Headquarters and the responsible region(s) to issue a cancellation notification by standard procedure to appropriate FEMA officials and FRP agencies. FRP agencies disengage according to standard procedure.

If an act of terrorism occurs that results in major consequences, each FRP component (the EST, CDRG, ROC, and DFO if necessary) disengages at the appropriate time according to standard procedure. Following FRP disengagement, operations by individual federal agencies or by multiple federal agencies under other federal plans may continue, in order to support the affected state and local governments with long-term hazard monitoring, environmental decontamination, and site restoration (cleanup).

RADIOLOGICAL ISOTOPES AND NUCLEAR WEAPONS

The Federal Radiological Emergency Response Plan (FRERP) covers any peacetime radiological emergency that has actual, potential, or perceived radiological consequences within the United States, its Territories, possessions, or territorial waters and that could require a response by the federal government. The level of the federal response to a specific emergency will be based on the type and/or amount of radioactive material involved, the location of the emergency, the impact on or the potential for impact on the public and environment, and the size of the affected area. Emergencies occurring at fixed nuclear facilities or during the transportation of radioactive materials, including nuclear weapons, fall within the scope of the Plan regardless of whether the facility or radioactive materials are publicly or privately owned, federally regulated, regulated by an Agreement state, or not regulated at all.

For fixed facilities and materials in transit, responses to radiological emergencies generally do not depend on the initiating event. The coordinated response

to contain or mitigate a threatened or actual release of radioactive material would be essentially the same whether it resulted from an accidental or deliberate act. For malevolent acts involving improvised nuclear or radiation dispersal devices, the response is further complicated by the magnitude of the threat and the need for specialized technical expertise/actions. Therefore, sabotage and terrorism are not treated as separate types of emergencies; rather, they are considered a complicating dimension of the emergency. The Atomic Energy Act directs the FBI to investigate all alleged or suspected criminal violations of the Act. Additionally, the FBI is legally responsible for locating any nuclear weapon, device, or material and for restoring nuclear facilities to their rightful custodians. In view of its unique responsibilities under the Atomic Energy Act, the FBI has concluded formal agreements with the LFAs that provide for interface, coordination, and technical assistance in support of the FBI's mission.

Generally, for fixed facilities and materials in transit, the designated LFA and supporting agencies will perform the functions delineated in this plan and provide technical support and assistance to the FBI in the performance of its mission. It would be difficult to outline all the possible scenarios arising from criminal or terrorist activity. As a result, the federal response will be tailored to the specific circumstances of the event at hand. For those emergencies where an LFA is not specifically designated (e.g., improvised nuclear device), the federal response will be guided by the established interagency agreements and contingency plans. In accordance with these agreements and plans, the signatory agency(ies) supporting the FBI will coordinate and manage the technical portion of the response and activate/request assistance under the FRERP for measures to protect the public health and safety. In all cases, the FBI will manage and direct the law enforcement and intelligence aspects of the response coordinating activities with appropriate federal, state, and local agencies within the framework of the FRERP and/or as provided for in established interagency agreements or plans.

In a response to an emergency involving a radiological hazard, the LFA under the FRERP is responsible for federal oversight of activities on site and federal assistance to conduct radiological monitoring and assessment and develop protective action recommendations. When a radiological emergency warrants action under the Stafford Act, FEMA uses the FRP to coordinate the nonradiological response to consequences off site in support of the affected state and local governments. If the FRERP and FRP are implemented concurrently, the Federal On-Scene Commander under the FRERP coordinates the FRERP response with the FCO, who is responsible for coordination of all federal support to state and local governments.

EMERGENCY TEAMS AND FACILITIES: AN OVERVIEW

The FRP and its operational components are designed to be flexible in order to accommodate the response and recovery requirements specific to the disaster. In

general, headquarters-level components provide support to the regional-level components that implement the on-scene operations in the field. Major components include:

The National Emergency Coordination Center (NECC) serves as FEMA's official notification point of an impending or actual disaster or emergency. This facility maintains a 24-hour capability to monitor all sources of warning/disaster information, including other federal agencies, FEMA regions, and the news media. The NECC reports disaster events to FEMA key officials, FEMA regions, and FRP signatory agencies. Each FEMA region is supported by a Mobile Emergency Response Support (MERS) Operations Center (MOC). Each MOC operates 24 hours a day and is tasked with monitoring events and providing pertinent information to FEMA regional staff and the NECC.

The Regional Operations Center (ROC) staff coordinates federal response efforts until an Emergency Response Team (ERT) is established in the field and the FCO assumes coordination responsibilities. Generally operating from the FEMA Regional Office, the ROC establishes communications with the affected state emergency management agency and the EST; coordinates deployment of the Emergency Response Team — Advance Element (ERT-A) to field locations; assesses damage information and develops situation reports (under ESF #5 — Information and Planning); and issues initial mission assignments. The ROC is activated by the FEMA Regional Director based on the level of response required. It is led by a ROC Director and consists of FEMA staff and ESF representatives, as well as a Regional Emergency Preparedness Liaison Officer (REPLO) who assists in coordination of requests for military support.

The Emergency Response Team — Advance Element (ERT-A) is the initial federal group that responds to an incident in the field. It is headed by a team leader from FEMA and is composed of FEMA program and support staff and representatives from selected ESF primary agencies. A part of the ERT-A deploys to the State Emergency Operations Center (EOC) or to other locations to work directly with the state to obtain information on the impact of the event and to identify specific state requests for federal response assistance that are called back to the ROC for processing. Other elements of the ERT-A (including MERS personnel and equipment) deploy directly to or near the affected area to establish field communications, locate and establish field facilities, and set up operations. The ERT-A identifies or validates the suitability of candidate sites for the location of mobilization center(s) and the DFO.

In a catastrophic disaster or high-visibility incident that would demand the full capabilities of FEMA, a National Emergency Response Team (ERT-N) may deploy to the affected area. The Director of FEMA determines the need for an ERT-N deployment, coordinating the plans with the affected region and other federal agencies. The ERT-N comprises staff from FEMA Headquarters and regional offices as well as other federal agencies. (Three ERT-N teams are rostered; each team is on call every third month.)

The Disaster Field Office (DFO) is the primary field location in each affected state for the coordination of federal response and recovery operations. It operates 24 hours per day, as needed, or under a schedule sufficient to sustain federal operations. The FCO and SCO collocate at the DFO, along with federal agency regional representatives and state and local liaison officers, when possible. Once the DFO is ready for use, the ERT-A and/or ERT-N is augmented by FEMA and other federal agency staff to form a full ERT.

The Emergency Response Team (ERT) is the principal interagency group that supports the FCO in coordinating the overall federal disaster operation. Located at the DFO, the ERT ensures that federal resources are made available to meet state requirements identified by the SCO. The size and composition of the ERT can range from FEMA regional office staff who are primarily conducting recovery operations to an interagency team having representation from all ESF primary and support agencies undertaking full response and recovery activities. The FCO's immediate staff can include a Deputy FCO and/or Deputy FCO for Mitigation as well as representatives providing assistance in the following organizational or functional areas: Equal Rights, Safety Officer, Environmental Officer, General Counsel, Emergency Information and Media Affairs, Congressional and Legislative Affairs, Community Relations, Office of the Inspector General, and Comptroller. In addition, a Defense Coordinating Officer works closely with the FCO or designated representative in orchestrating military support. The Operations section coordinates the delivery of federal assistance and manages the activities of various emergency teams. Immediate support staff functions include Mission Assignment Coordination, Action Tracking, Defense Coordinating Element, and Mobile Emergency Response Support. The section is composed of four branches — Operations Support, Human Services, Infrastructure Support, and Emergency Services. The 12 ESFs, along with several recovery program groups, are organized functionally under the branches to provide a coordinated approach and ensure seamless delivery of assistance to disaster survivors and the affected state. The Information and Planning section has two major tasks: the collection, processing, analysis, and dissemination of information about disaster operations to support planning and decision making at both the field operations and headquarters levels; and the coordination of short- and long-term planning at the field operations level. The Logistics section plans, organizes, and directs logistics operations that include control and accountability for supplies and equipment; resource ordering; delivery of supplies, equipment, and services to the DFO and other field locations; resource tracking; facility location, setup, space management, building services, and general facility operations; transportation coordination and fleet management services; information and technology systems services; administrative services such as mail management and reproduction; and customer assistance. The Administration section is responsible for personnel functions and employee services. Personnel functions cover tracking FEMA staff and disaster reservist deployment, obtaining local hires, arranging billeting, and processing payroll. Employee services include providing for ERT personnel health and safety, over-

seeing access to medical services, and ensuring security of personnel, facilities, and assets.

The Emergency Support Team (EST) is the interagency group that provides general coordination support to the ROC staff, ERT-A, and ERT response activities in the field. Operating from the FEMA Emergency Information and Coordination Center (EICC) in Washington, DC, the EST is responsible for coordinating and tracking the deployment of Initial Response Resources, DFO kits, Disaster Information Systems Clearinghouse (DISC) packages, and other responder support items to the field. The EST serves as the central source of information at the headquarters level regarding the status of ongoing and planned federal disaster operations. The EST attempts to resolve policy issues and resource support conflicts forwarded from the ERT. Conflicts that cannot be resolved by the EST are referred to the CDRG. The EST also provides overall resource coordination for concurrent multi-state disaster response activities. ESF primary agencies send staff to the EST or opt to coordinate response support activities from their own agency EOCs. The EST organizational structure parallels the ERT organization, but is not identical.

The Catastrophic Disaster Response Group (CDRG), composed of representatives from all FRP signatory departments and agencies, operates at the national level to provide guidance and policy direction on response coordination and operational issues arising from the FCO and ESF response activities. CDRG members are authorized to speak for their agencies at the national policy level. During a disaster the CDRG convenes as necessary, normally at FEMA Headquarters; the EST provides any needed support.

A Disaster Recovery Center (DRC) is a centralized location where individuals affected by a disaster can go to obtain information on disaster recovery assistance programs from various federal, state, and local agencies as well as voluntary organizations. Trained staff also is on hand to provide counseling and advice. It is generally expected that individuals visit the DRC after they have called the tele-registration center to apply for assistance, as applications usually will not be taken at the DRC. However, a DRC may serve as a workshop site for assisting families and businesses to complete Small Business Administration disaster loan application forms. A center dealing only with mitigation in reconstruction and rebuilding techniques may be called a Reconstruction Information Center (RIC). A RIC may be set up at a fixed or mobile location.

Additional specialized teams are ready for deployment to support disaster operations, including damage assessment teams, Disaster Medical Assistance Teams, Donations Coordination Teams, Urban Search and Rescue (US&R) task forces, US&R Incident Support Teams, and mitigation assessment teams. Additional facilities support organizational deployment, including assembly points, mobilization centers, staging areas, points of departure, and points of arrival. Various other coordinating mechanisms, management tools, and information systems contribute to the overall federal disaster operations system. The Time-Phased Force and Deployment List (TPFDL) is a tool to manage the rapid, systematic

movement of federal response personnel, equipment, and critical relief supplies into an affected area in accordance with operational priorities. The Movement Coordination Center (MCC) is an element under ESF #1 that is located at FEMA Headquarters and, if necessary, in the field to coordinate the acquisition of transportation capacity and maintain visibility over validated transportation requests for assistance from inception through delivery to a mobilization center. The Rapid Response Information System (RRIS) is a system of databases and links to Internet sites providing information to federal, state, and local emergency officials on federal capabilities to render assistance to manage the consequences of a terrorist attack using weapons of mass destruction. This information is directly available to designated officials in each state, the FEMA regions, and key federal agencies via a protected Intranet site. Local officials have access to the abbreviated Internet site and indirectly to the Intranet site through their state counterparts. Additional information is available to the emergency response community on characteristics of weapons of mass destruction and appropriate safety measures; availability of excess or surplus federal equipment; access to chemical, biological, and nuclear helplines and hotlines; training courses; and a reference library.

The following overview illustrates response and recovery actions federal agencies likely will take to help state and local governments that are overwhelmed by a major disaster or emergency. Key operational components that could be activated include the Regional Operations Center (ROC), Emergency Response Team — Advance Element (ERT-A), National Emergency Response Team (ERT-N), Emergency Support Team (EST), Emergency Response Team (ERT), Disaster Field Office (DFO), Catastrophic Disaster Response Group (CDRG), and Disaster Recovery Center (DRC).

1. FEMA's National Emergency Coordination Center continually monitors potential disasters and emergencies. When advance warning is possible, FEMA may deploy, and may direct federal agencies to deploy liaison officers and personnel to a State Emergency Operations Center to assess the emerging situation. A ROC may be activated, fully or partially. Facilities, such as mobilization centers, may be established to accommodate personnel, equipment, and supplies.

2. Immediately after a disaster, local jurisdictions respond using available resources and notify state response elements. As information emerges, they also assess the situation and request state assistance if needed. The state reviews the situation, mobilizes state resources, and informs the FEMA Regional Office of actions taken. The Governor declares a state of emergency, activates the state emergency operations plan, and requests a Presidential disaster declaration. The state and FEMA jointly conduct a Preliminary Damage Assessment to validate the state's request and determine the kind of federal assistance needed.

3. After the declaration, a ROC, staffed by regional personnel, coordinates initial regional and field activities such as deployment of an ERT-A. The ERT-A assesses the impact of the event, gauges immediate state needs, and makes preliminary arrangements to set up operational field facilities. (If regional resources

appear to be overwhelmed or if the event has potentially significant consequences, FEMA may deploy an ERT-N.)

4. An interagency EST, composed of Emergency Support Function (ESF) representatives and FEMA support staff, carries out initial activation and mission assignment operations and supports the ROC from FEMA Headquarters.

5. A Federal Coordinating Officer (FCO), appointed by the FEMA Director on behalf of the President, coordinates federal activities. The FCO works with the State Coordinating Officer to identify requirements.

6. The FCO heads the interagency ERT. The ERT works with the affected state and conducts field operations from the DFO. ESF primary agencies assess the situation and identify requirements. Under FEMA mission assignments or their own authorities, agencies supply goods and services to help the state respond effectively.

7. The CDRG, composed of representatives from FRP signatory agencies, convenes at FEMA Headquarters when needed to provide guidance and policy direction on coordination and operational issues. The EST supports the CDRG and coordinates with the ERT.

8. As immediate response priorities are met, recovery activities begin in the field. federal and state agencies helping with recovery and mitigation convene to discuss state needs.

9. Teleregistration is activated and has a toll-free telephone number disaster victims can call to apply for assistance. A toll-free disaster helpline is established to answer common questions. One or more DRCs may be opened where victims can obtain information about disaster assistance, advice, and counsel. The affected area is inspected to determine the extent of damage, and funds for approved assistance are obligated.

10. Concurrently, Applicant Briefings are conducted for local government officials and certain private nonprofit organizations to inform them of available assistance and how to apply. Applicants must first file a Request for Public Assistance. Eligible applicants will then be notified and will define each project on a Project Worksheet, which details the scope of damage and a cost estimate for repair to a pre-disaster condition. The Project Worksheet will be used as the basis for obligating funds to the state for eligible projects.

11. Throughout response and recovery, mitigation staff at the DFO examines ways to maximize mitigation measures. Hazard Mitigation Site Survey Teams contact local officials to identify potential projects and suggest which ones should be included in an early implementation strategy. The strategy, produced in cooperation with federal, state, and local officials, focuses on viable opportunities to provide funds, technical assistance, and staff support to incorporate mitigation into the repair and replacement of damaged or destroyed housing and infrastructure.

12. As the need for full-time interagency coordination at the DFO ceases, the ERT plans for selective release of federal resources, demobilization, and closeout. federal agencies then work directly with their grantees from their re-

gional or headquarters offices to administer and monitor individual recovery programs, support, and technical services.

CHEMICAL EXAMPLE: HAZMAT FIRE IN BALTIMORE TUNNEL

An accident involving a 60-car CSX freight train in the 1.7-mile Howard Street Tunnel in downtown Baltimore occurred July 18, 2001 at 3:07 PM local time. More than 125 firefighters worked for hours to contain the blaze involving eight cars with numerous hazardous chemicals including hydrochloric acid, acetic acid, propylene glycol, tripropylene, and ethyl hexyl phthalate. The skin irritation resulting from these chemicals made reaching the tunnel fire extremely difficult. Not until late evening, after fighting the fire from a distance for several hours, could firefighters approach the fire from within the tunnel; it took about eight hours for firefighters to reach the burning train cars. The temperature just several feet in from the south entrance of the tunnel was 400 degrees, and an estimated 1500 degrees further in. As of midnight, it was determined that the fire caused a water main break which occurred later that evening above the tunnel, resulting in the flooding of numerous city streets and leaving approximately 1,200 customers, mainly businesses, without electricity. A major MCI WorldCom fiber optic cable had been severed in the tunnel, resulting in phone and Internet outages for some regional customers. Verizon and MCI both confirmed service disruptions and outages in the northeast due to damaged cables in the tunnel. Effects of the damage were felt by Internet and cellular phone users throughout the eastern U.S. Two firefighters and at least twenty others were treated at area hospitals, most for chest pains, respiratory problems, and eye irritation. Weather conditions were favorable for keeping smoke away from nearby densely populated areas. As of midnight Wednesday night, major roadways were reopened but a great deal of traffic trouble had occurred throughout the day Thursday. There was one tanker leaking hydrochloric acid in the tunnel. CSX transferred the acid from the damaged tanker into an empty tanker before removing it from the tunnel, a six to seven hour process. Officials kept people at least one block from the scene due to concerns that the damaged road might buckle. Water and electricity was restored to all customers by Thursday. About 50 trains a day used CSX's Howard Street Tunnel and its closure created logistical problems for many northeast companies. Shippers scrambled to find other means of transportation; either by Norfolk Southern or trucking companies as a temporary solution. By Friday, officials reported that the fire likely began in the train car which carried tripropylene where a spark could have ignited the leaking chemical. A tank car leaking hydrochloric acid was pumped out after leaking between 8,000 and 10,000 gallons since the Wednesday derailment. Phone service and Internet was restored by Sunday. Monday morning at 7:10 AM, the tunnel fire was declared under control. The tunnel was then vented to remove high levels of carbon monoxide. A group of inspectors, including a CSX bridge maintenance engineer, Federal Railroad Administration (FRA) officials, Baltimore city engineers, and Baltimore Mass Transit Administration (MTA) officials, entered

the Howard Street Tunnel Monday evening for the first damage assessment. Respirators were required due to the carbon monoxide still escaping from the 1.5 mile tunnel. A test train with approximately 50 cars was taken through the tunnel late Monday morning. CSX operated another additional train through the tunnel Monday evening. CSX resumed freight service through the Howard Street Tunnel on Tuesday at limited speed after a night and day of cleanup efforts and laying of new track. CSX and the City of Baltimore have continued their talks with one another regarding the expenses involved in the cleanup and recovery efforts. More than two dozen damage claims have been filed with CSX by local businesses affected by the incident. CSX has agreed to pay \$1.3 million to the city in overtime for Baltimore firefighters and police officers involved in the derailment. This incident never rose above a state level response.

BIOLOGICAL EXAMPLE: TOPOFF 2000 EXERCISE, DENVER, CO

The U.S. Congress, in an effort "to assess the nation's crisis and consequence management capacity under extraordinarily stressful conditions," directed the Department of Justice to conduct an exercise engaging key personnel in the management of mock chemical, biological, or cyber terrorist attacks. The resulting exercise was called TOPOFF; the name stems from the engagement of top officials of the U.S. government. TOPOFF was a \$3 million dollar drill testing the readiness of top government officials to respond to terrorist attacks at multiple geographic locations. It was the largest exercise of its kind to date. The exercise took place in May 2000 in three U.S. cities, and portrayed a chemical weapons event in Portsmouth, NH, a radiological event in the greater Washington, D.C. area, and a bioweapons event in Denver, CO. The bioterrorism component of the exercise centered on the release of an aerosol of *Yersinia pestis*, the bacteria that causes plague. Denver was selected in part because it had received Domestic Preparedness training and equipment. The following is the chronology of simulated events for the bioterrorism component of the exercise. **May 17:** An aerosol of plague (*Y. pestis*) bacilli is released covertly at the Denver Performing Arts Center. **May 20 (Day 1 of exercise):** The Colorado Department of Public Health and Environment receives information that increasing numbers of persons begin seeking medical attention at Denver area hospitals for cough and fever during the evening of May 19th. By early afternoon on May 20th, 500 persons with these symptoms have received medical care, 25 of whom have died. The Health Department notifies the CDC of the increased volume of sick. Plague is confirmed first by the state laboratory and subsequently confirmed in a patient specimen by the CDC lab at Ft. Collins. A public health emergency is declared by the State Health Officer. The state Health officer places an official request for support from DHHS's Office of Emergency Preparedness. The Governor's Emergency Epidemic Response Committee assembles to respond to the unfolding crisis. Thirty-one CDC staff are sent to Denver. The CDC is notified by Denver police and the FBI that a dead man has been found with terrorist literature and paraphernalia in his possession; his cause

of death is unknown. Hospitals and clinics around the Denver area who just a day ago were dealing with what appeared to be an unusual increase in influenza cases are recalling staffs, implementing emergency plans, and seeking assistance in determining treatment protocols and protective measures. By late afternoon, hospital staff are beginning to call in sick, and antibiotics and ventilators are becoming more scarce. Some hospital staff have donned respiratory protective equipment. The Governor issues an Executive Order that restricts travel - including bus, rail and air travel - into or out of 14 Denver Metro counties, and commandeers all antibiotics that can be used to prevent or treat plague. During a VNN press conference where a number of agencies are represented, the Denver public is informed that there is a plague outbreak in the city following a terrorist attack and is told of the governor's Executive Order. Citizens are told to seek treatment at a medical facility if feeling ill or if they have been in contact with a known or suspected case of plague. Those who are well are directed to stay in their homes and avoid public gatherings. The public is told that the disease is spread from person to person only "if you are within 6 feet of someone who is infected and coughing" and told that dust masks are effective at preventing the spread of disease. Confirmed cases of plague are identified in Colorado locations other than Denver. Patient interviews suggest that most victims were at the Performing Arts Center days earlier. It is announced that the governor is working with the President of the United States to resolve the crisis and that federal resources are being brought in to support of state agencies. By the end of the day, 783 cases of pneumonic plague have occurred; 123 persons have died. **May 21** (Day 2 of exercise): VNN reports that a "national crash effort" is underway to move large quantities of antibiotics to the region as the CDC brings in its "national stockpile", but the quantity of available antibiotics is uncertain. The report explains that early administration of antibiotics is effective in treating plague but that antibiotics must be started within 24 hours of developing symptoms. A VNN story a few hours later reports that hospitals are running out of antibiotics. A "Push-Pack" from the National Pharmaceutical Stockpile (NPS) arrives in Denver, but there are great difficulties moving antibiotics from the stockpile delivery point to the persons who need it for treatment and prophylaxis. Out of state cases begin to be reported. The CDC notifies bordering states of the epidemic. Cases are reported in England and Japan. Both Japan and the World Health Organization (WHO) request technical assistance from the CDC. A number of hospitals in Denver are full to capacity and by the end of the day are unable to see or admit new patients. Thirteen hundred ventilators from the NPS are to be flown to Colorado. Bodies in hospital morgues are reported to have reached critical levels. By 5 pm, the CDC has carried out an epidemiological investigation on 41 cases. The U.S. Surgeon General flies to Colorado to facilitate communications issues. Many states now are requesting that they receive components of the NPS from the CDC. By the end of the day, 1,871 plague cases have occurred throughout the U.S., London and Tokyo. Of these, 389 persons have died. **May 22** (Day 3 of exercise): Hospitals are under-staffed and have insufficient antibiotics, ventilators, and beds to meet demand. They cannot manage the influx of sick patients into

the hospitals. Medical care is "beginning to shut down" in Denver. One hundred fifty-one patient charts have been reviewed by state and federal health officials pursuing the epidemiological investigation. There are difficulties getting antibiotics from the National Stockpile to the facilities that need them. Details of a distribution plan are still not formalized. Officials from the Health Department and the CDC have determined that secondary spread of disease appears to be occurring. The population in Denver is encouraged to wear face masks. The CDC advises that Colorado state borders be cordoned off in order to limit further spread of plague throughout the U.S. and other countries. Colorado officials express concern about their ability to get food and supplies into the state. The governor's executive order is extended to prohibit travel into or out of the state of Colorado. By noon, there are 3,060 U.S. and international cases of pneumonic plague, 795 of whom have died. **May 23** (Day 4 of exercise): There are conflicting reports of the number of sick and dead. Some reports show an estimated 3,700 cases of pneumonic plague with 950 deaths. Others are reporting over 4,000 cases and more than 2,000 deaths. The TOPOFF Exercise is terminated.

RADIOLOGICAL EXAMPLE: THREE MILE ISLAND (TMI) ACCIDENT

TMI: Response to the accident was swift. The NRC's regional office in King of Prussia, Pennsylvania, was notified at 7:45 a.m. on March 28, 1979. By 8:00, the NRC headquarters in Washington, D.C. was alerted and the NRC Operations Center in Bethesda, Maryland, was activated. The regional office promptly dispatched the first team of inspectors to the site and other agencies, such as the Department of Energy, and the Environmental Protection Agency, also mobilized their response teams. Helicopters hired by TMI's owner, General Public Utilities Nuclear, and the Department of Energy were sampling radioactivity in the atmosphere above the plant by midday. A team from the Brookhaven National Laboratory was also sent to assist in radiation monitoring. At 9:15 a.m., the White House was notified and at 11:00 a.m., all non-essential personnel were ordered off the plant's premises. From the early stages of the accident, low levels of radioactive gas, mostly in the form of xenon, continued to be released to the environment. At the time, efforts to halt the releases were unsuccessful and there was some fear of an explosion from the buildup of hydrogen - -fortunately, this did not occur. However, on Friday, March 30, Governor Thornburgh of Pennsylvania ordered a precautionary evacuation of preschool children and pregnant women from within the 5-mile zone nearest the plant, and suggested that people living within 10 miles of the plant stay inside and keep their windows closed. Most evacuees had returned to their homes by April 4. By that time, the situation at the reactor had been brought under control. The American Nuclear Insurers, an organization made up of nuclear insurance firms, had already begun distributing checks to evacuees to cover hotel and meal expenses, and was beginning to handle claims for property and liability losses.

CONCLUSIONS

The National Response Plan is a work in progress. The elements of this plan have been outlined as of the time of this writing. These elements will evolve and the reader should use this document only as a roadmap to understanding the processes involved.

24

Emergency Response and Training

Robb L. Pilkington

University of Missouri, Columbia, Missouri

INTRODUCTION

Emergency response to a terrorism incident always begins at the local level escalating to the next higher level of government as resources are consumed. Regardless of what type of event has occurred, common response requirements must be met such as scene security, sheltering or evacuation of individuals, medical care for victims and responders, temporary feeding of displaced individuals and responders, etc. Because the response will require the assistance and support from every department of local government, the key to success is prior planning, identification of available resources and shortfalls, local response training and practice (exercises). This cycle of planning, training and exercise should be ongoing and incorporate changes in technology, federal and state planning, and recommendations for improvement from exercise participants (See Figure 24.1).

EMERGENCY RESPONSE PLANNING

The Federal Response Plan (FRP) maintained by the Federal Emergency Management Agency is the framework by which the federal government responds to emergencies and disasters. The premise behind the FRP is that regardless of what type of emergency or disaster occurs, there are twelve common response and recovery functions required to limit or prevent human suffering and limit property damage. The Emergency Support Functions (ESF) are assigned a primary agency responsible for planning and implementing the required services; and supporting agencies which are tasked to assist through the provision of resources and personnel.

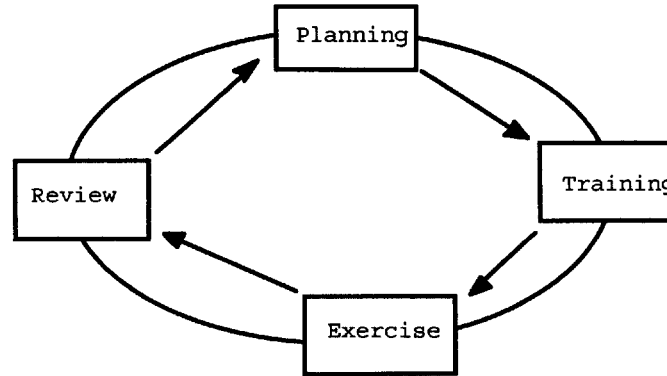


Figure 24.1 The Emergency Response Preparedness Cycle.

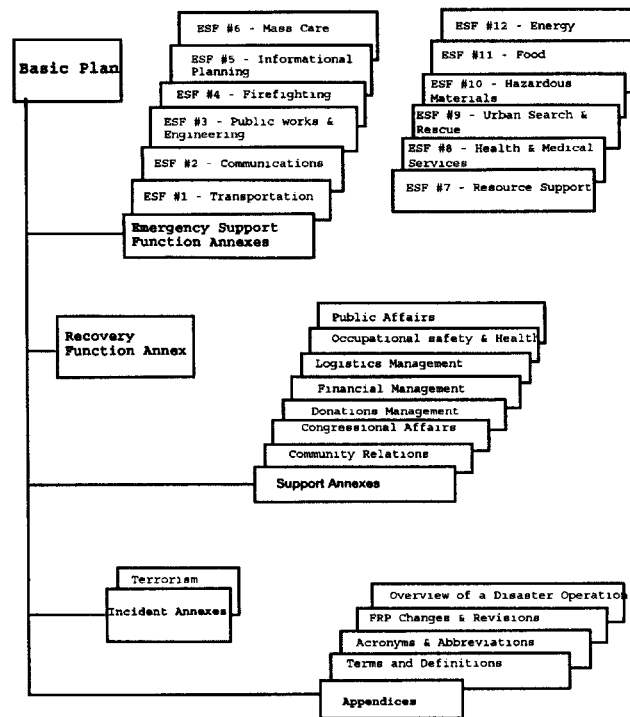


Figure 24.2 Organization of the FRP and the twelve Emergency Support Functions. (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

Figure 24.2 shows the organization of the FRP and the twelve Emergency Support Functions. Note that Terrorism is a separate annex in the FRP.

Local and State Governments for the most part have adopted a similar emergency response plan frame work, modifying the ESF concept to conform to state and local governmental divisions and differences in organizations.

The relationship of local state, federal, volunteer, and international organizations in planning for an emergency or disaster is diagramed below (Figure 24.3).

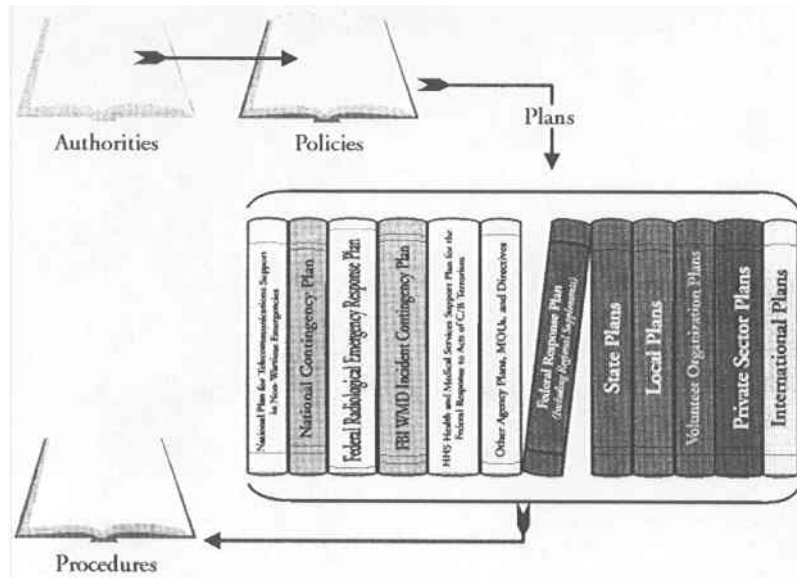


Figure 24.3 The relationship of local, state, federal, volunteer, and international organizations in planning. (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

The FEMA disaster response model is presented to demonstrate the coordination requirements and the number of agencies involved with emergency and disaster operations. This additionally diagrams the disaster cycle from the initial incident through response, recovery and disaster mitigation. This model is shown in Figure 24.4.

ADDITIONAL PLANNING FOR A TERRORIST EVENT

Unlike natural disasters, a terrorism event represents a willful attack against the United States and is therefore a criminal act. Presidential Decision Directive 39 (PDD-39) and the amplifying PDD-62 direct the US Department of Justice, Federal Bureau of Investigation to assume the responsibility as the Lead Federal Agency (LFA) in disasters and emergencies where terrorism is suspected. As this

is a departure from normal disaster operations planning, separate plans (annexes) have been developed to facilitate the coordination of resources and personnel. FEMA acts in a support role to the FBI during the response or “*Crisis Phase*” of a terrorism incident. When the FBI has finished collecting evidence and processing the “*Crime Scene*”, FEMA becomes the Lead Federal Agency for recovery (*Consequence Phase*). There is a period of overlap between the Crisis and Consequence Phases in which both the FBI and FEMA coordinate crime scene and life/safety/recovery issues. The relationship between Crisis and Consequence Management for a WMD / Terrorist event is depicted below in Figure 24.5.

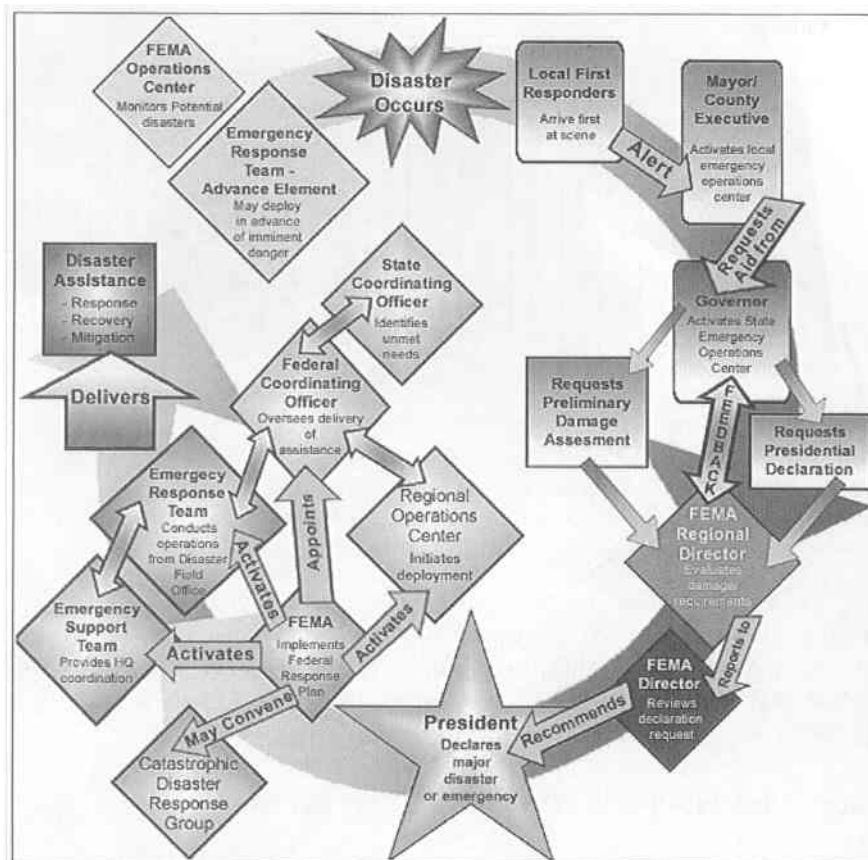


Figure 24.4 The FEMA model. (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

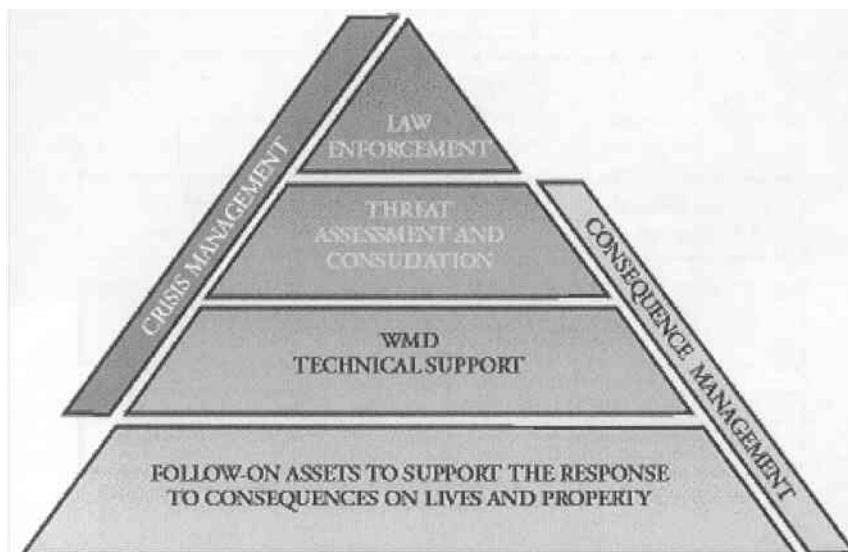


Figure 24.5 Management of a WMD/Terrorist event. (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

The FBI Crisis Management Plan for responding to a terrorist incident is contained in two planning documents titled: “Chemical / Biological Incident Contingency Plan” and the “Radiological Incident Contingency Plan”. The plans contain specific incident management requirements and denote organizational relationships between Local, State and Federal Agencies. It should be noted that the FBI uses a different management model than FEMA uses in their response to natural or technological emergencies (see Figure 24.6).

The chart below (Figure 24.7) denotes the incident management system used by the FBI and FEMA to coordinate Crisis and Consequence operations. The organizations and individuals listed below will be co-located in a Joint Operations Center (JOC) near where the incident occurred. The Operations Group is responsible for the criminal investigation side of a WMD incident; the Consequence Management Group is responsible for assisting individuals, businesses and the affected community recover from the attack.

A senior FBI agent heads the Command Group with assistance from representatives from FEMA, State Government and Local Response Agencies.

The Support Group provides Administrative, Logistics and Communication support to both the Operations and the Consequence Management Groups.

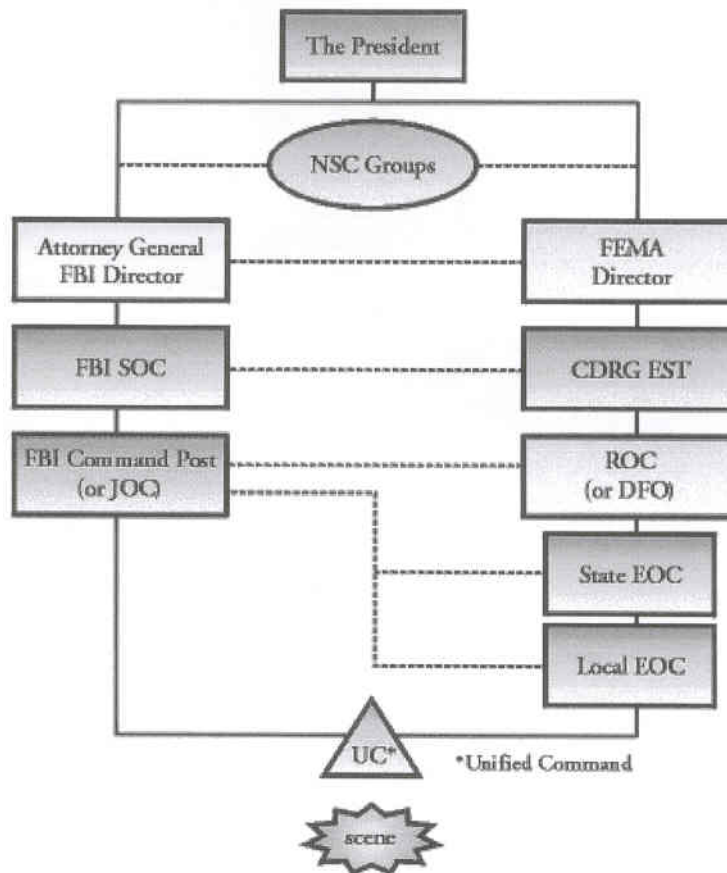


Figure 24.6 FBI Response Organization for Terrorism Incidents:

Note: there is a parallel organizational chain of command for the FBI and FEMA with the National Security Council (NSC) and the President monitoring the status of the response. The role of the NSC is to coordinate counter-terrorism activities within and outside the United States. (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

A senior FEMA official designated by the President as the Federal Coordinating Officer (FCO) supervises the Consequence Management Group. Support agencies and activities are as stipulated in the Federal Response Plan.

The majority of FRP agencies will be located in a separate facility with liaison officers assigned to the Joint Operations Center. The FEMA designation for this facility is the Disaster Field Office (DFO), and will serve as the sight for sustained consequence management operations once the FBI (Crisis Management) role is concluded. The DFO may be staffed for several months or longer depending upon the magnitude of human loss and infrastructure damage.

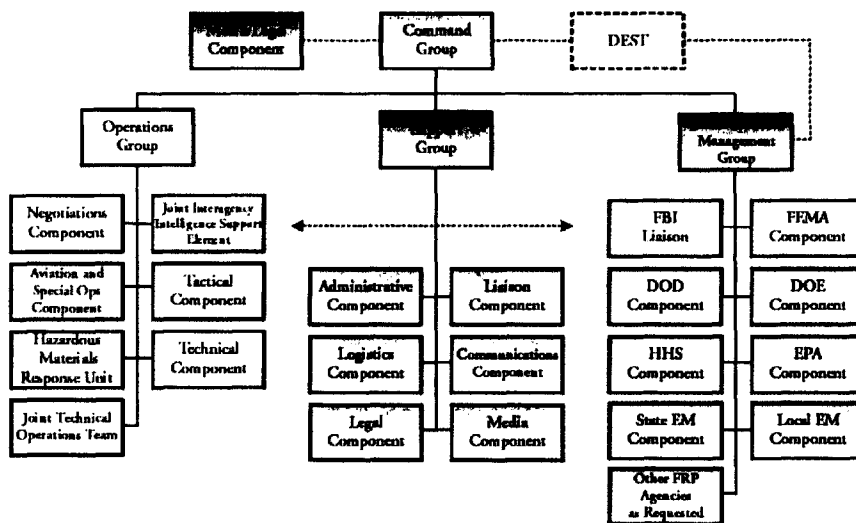


Figure 24.7 Incident management structure (Source: Federal Emergency Response Plan, Federal Emergency Management Agency).

LOCAL RESPONSE – A TEAM APPROACH

The effectiveness of the local response to a terrorism event is dependent upon the capabilities, available resources and level of training of each department or agency. Critical to the response however is the ability to coordinate activities and anticipate requirements, and familiarity with the local response plan.

The Department of Justice, Office of Justice Programs developed a list of response functions by agency to assist local jurisdictions evaluate their capability to respond to a Weapons of Mass Destruction (WMD) event. The following chart (Figure 24.8) identifies the functional differences between responding disciplines.

It can be generally assumed that the capabilities of departments in large metropolitan areas will greatly exceed those of small rural communities. Larger communities tend to have specialized teams for hazardous material, explosive and armed criminal incidents. Smaller communities rely on shared resources or mutual aid assistance from adjacent jurisdictions. It is not uncommon for the closest hazardous materials capable response team or a level I trauma center to be located 1-2 hours away. This demonstrates the need for detailed prior planning, identification of resources and practice prior to an actual terrorist incident.

The number of personnel, the level of training and the type and amount of equipment a response organization has available measures response capability to a WMD incident. The Department of Justice categorizes WMD response capability

in four Tiers (I-IV), with Tier I having the least capability and training and Tier IV representing an organization that is highly skilled and self-sufficient. It is important to note that an effective response capability must contain both equipment and trained personnel.

Agency	Fire Service	HazMat	EMS	Law Enforcement	Public Works	Public Health	Emergency Management
Duties & Functions (sample - not an all inclusive list)	Recognize HazMat Situations	Stop Leak Contain Spill	Recognize HazMat Situations	Recognize HazMat Situations	Recognize HazMat Situations	Conduct Mass Casualty Operations	Command Post Operations
	Self Protection	Consultation and Support to Unified Command	Self Protection	Self Protection	Self Protection	Care for Grossly Decontaminated Patients	Consultation and Support to Unified Command
	Unified Command	Decontaminate own Employees (HazMat Team)	Care and Transport of Grossly Decontaminated Patients	Scene Security	Unified Command	Diagnose and Treat Chemical, Biological and Radiological Injuries	Communications
	Access Data about Material Involved	Decontaminate Victims	Patient Decontamination	Mobile Command Post Operations	Unified Command	Recognize Potential WMD Terrorism Incidents	Recognize Potential WMD Terrorism Incident
	Access HazMat Team	May Provide EMS Support for Own Team	Immediate Treatment of WMD Patients	Communications	Communications	Self Protection	
	Patient Decontamination	Communications	Transport WMD Patients	Recognize Potential WMD Terrorism Incidents	Recognize Potential WMD Terrorism Incidents	Unified Command	
	Communications	Recognize Potential WMD Terrorism Incidents				Consultation and Support to Unified Command	
	Mobile Command Post Operations	Identify Contaminated Area				Medical Surveillance	
	Recognize Potential WMD Terrorism Incidents					Agent Diagnosis	
						Communications	

Figure 24.8 Response Functions for Emergency Responders. (Source: US Department of Justice, Office of Justice Programs, Office of Domestic Preparedness).

Tier I represents the basic level of training and types of operations every community should achieve. This level facilitates recognition of a WMD event and the implementation of protective measures such as evacuation. The community does not have the capability to stop the release of chemicals or biological agents, defuse a bomb, mitigate radiological dispersal incidents or medically treat large numbers of victims. It relies on outside assistance from other communities, the state and federal government for technical and medical support.

	Response Capability	Associated Equipment	Supporting Training Courses
Tier IV (Specialized Capability)	Tier III competency plus: <ul style="list-style-type: none"> • Ability to operate unhindered by equipment shortfalls in any contaminated environment 	<ul style="list-style-type: none"> • High Level Equipment • Advanced detection • Computer database references • Computer programming for detection equipment • Responder protected detection equipment 	<ul style="list-style-type: none"> • Specialist level HazMat • Specialist level Physician, Nurse, and Public Health
Tier III (Technician Capability)	Tier II competency plus: <ul style="list-style-type: none"> • Advanced knowledge of operations • Initial detection and monitoring • Establish mass casualty response/treatment systems • Establish transport for mass casualties • Conduct safe sampling procedures in contaminated environment 	<ul style="list-style-type: none"> • Moderate Increase Level Equipment • Level A, B, & C PPE 	<ul style="list-style-type: none"> • Technician Level HazMat • Selected EMS personnel • Selected Physician, Nurse, and Public Health personnel
Tier II (Operators Capability)	Tier I competency plus: <ul style="list-style-type: none"> • Operate with HazMat teams • Advanced PPE measures • Implement evacuation plans • Use decontamination and basic detection equipment 	<ul style="list-style-type: none"> • Modest Increase Level Equipment • Level B & C PPE • Self-Contained Breathing Apparatus 	<ul style="list-style-type: none"> • Tactical Emergency Medical Service Operations • Operations Level B Selected Fire, HazMat, EMS, Law, Public Works, and Public Health
Tier I (Basic Defensive Capability)	<ul style="list-style-type: none"> • Conduct defensive operations in a contaminated environment • Self protective measures • Protect general population from further contamination 		<ul style="list-style-type: none"> • Terrorism Awareness Course • Awareness Level B All disciplines

Figure 24.9 Capability Assessment Chart. (Source: US Department of Justice, Office of Justice Programs, Office of Domestic Preparedness).

Tier II and III communities are not self sufficient but do have the training, personnel and the equipment required to detect agents, mitigate explosives and radiological dispersal devices and treat contaminated injured victims. Outside assistance will still be required to make up shortfalls in personnel and equipment.

Tier IV represents a community, which has adequate resources and personnel to mitigate all but the largest conceivable WMD event. Only a handful of cities have this capability such as New York and Los Angeles.

It must be stressed that community capability is the summation of the number of trained personnel and type of equipment each individual agency has available to respond to an event. It is dependent upon each organization participating at a common level. A community in which the fire department is trained and has purchased necessary equipment but the emergency medical service has no interest in participating is not able to respond effectively as a team.

TERRORISM INCIDENT RESPONSE – TEMPLATES FOR SUCCESS

The following templates demonstrate the interrelationship of agencies and functions when responding to different WMD events. The templates are a compilation of emergency response plans and SOPs.

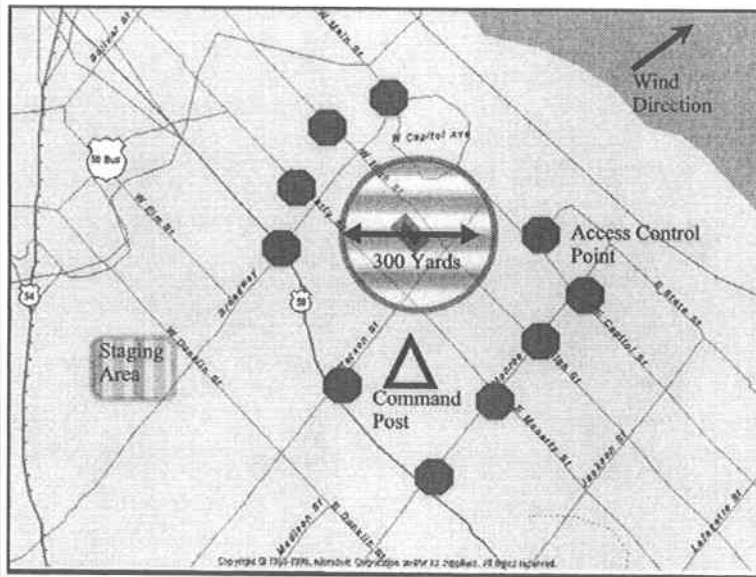


Figure 24.10 Generic Initial Response template.



The “Danger Area” or “Hot Zone” is an initial isolation area around the site of the incident. The size of the area is event dependent. If the emergency involves explosives, then the radius is determined by the type of device (pounds of explosive); if it is a chemical threat, the size is determined by a combination of factors including type of chemical, surrounding terrain and environmental factor such as wind, humidity, temperature and time of day.



This symbol represents access or traffic control points. These are roadblocks to prevent individuals from entering the scene. The security and traffic control points are initially the responsibility of law enforcement, but can be turned over to other agencies such as Parks Department or Public works to free up the law enforcement officers for additional duties or resumption of patrol.



The Command Post is where the incident command team assembles. The number of individuals is kept to a minimum to reduce confusion, noise and congestion.



The Staging Area is a designated location where Police, Fire, EMS and other responders are directed initially while the incident is being assessed. The Staging Area is relatively close to the scene, but far enough away to prevent congestion. As a resource is needed, the Command Post will relay instructions through a "Staging Officer".

The above generic scene diagram should readily demonstrate the following:

1. Access Control can quickly deplete on-duty law enforcement personnel. It is essential that Access Control assistance be readily available from other agencies such as the street department, adjacent law enforcement agencies or even park rangers, etc.
2. Staging areas must be preplanned and communicated quickly to arriving units.
3. The "Danger Area / Hot Zone" can encompass many hundreds of people if the scene is located in a downtown area. The decision to evacuate or shelter the affected population must take into account the type of incident, construction of adjacent buildings and the risk of moving individuals vs. keeping them inside with ventilation systems secured.
4. Communication is essential for notifying both the responders of command orders and for letting the public know what to do.

EXPLOSIVE INCIDENT RESPONSE TEMPLATE

The response to an incident involving suspected explosives requires limited number of personnel at the scene (to minimize injury should the device explode), and the use of bomb technicians and bomb search canines. Because many explosive detonators are sensitive to radio frequencies, all cellular telephones, radios and in some cases pagers must be turned off.

Most explosive incidents begin with an anonymous phone call or note. It is important that personnel who are responsible for answering telephone calls be trained in the proper procedures for receiving bomb threats. The validity of the threat can often be determined by the type and amount of information a caller reveals. The Bureau of Alcohol, Tobacco and Firearms has a Bomb Threat Checklist available to assist call-takers record information.



There is also a real threat that more than one explosive device has been planted. These "Secondary Devices" are usually outside and away from the initial

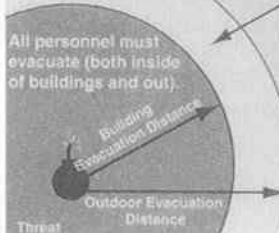
device, and are designed to explode and injure the first responders. A site security screening is necessary when establishing the command post and staging areas.

Terrorist Bomb Threat Stand-Off

THREAT	THREAT DESCRIPTION	EXPLOSIVES CAPACITY ¹ (TNT EQUIVALENT)	BUILDING EVACUATION DISTANCE ²	OUTDOOR EVACUATION DISTANCE ³
	PIPE BOMB	5 LBS/ 2.3 KG	70 FT/ 21 M	850 FT/ 259 M
	BRIEFCASE/ SUITCASE BOMB	50 LBS/ 23 KG	150 FT/ 46 M	1,850 FT/ 564 M
	COMPACT SEDAN	500 LBS/ 227 KG	320 FT/ 98 M	1,500 FT/ 457 M
	SEDAN	1,000 LBS/ 454 KG	400 FT/ 122 M	1,750 FT/ 534 M
	PASSENGER/ CARGO VAN	4,000 LBS/ 1,814 KG	640 FT/ 195 M	2,750 FT/ 838 M
	SMALL MOVING VAN/DELIVERY TRUCK	10,000 LBS/ 4,536 KG	860 FT/ 263 M	3,750 FT/ 1,143 M

This card supersedes any previous undated versions 11/99

THREAT	THREAT DESCRIPTION	EXPLOSIVES CAPACITY ¹ (TNT EQUIVALENT)	BUILDING EVACUATION DISTANCE ²	OUTDOOR EVACUATION DISTANCE ³
	MOVING VAN/ WATER TRUCK	30,000 LBS/ 13,608 KG	1,240 FT/ 375M	6,500 FT/ 1,982 M
	SEMI-TRAILER	60,000 LBS/ 27,216 KG	1,570 FT/ 475 M	7,000 FT/ 2,134 M



All personnel must either seek shelter inside a building (with some risk) away from windows and exterior walls, or move beyond the Outdoor Evacuation Distance.

Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors.

- 1 Based on maximum volume or weight of explosive (TNT equivalent) that could reasonably fit in a suitcase or vehicle.
- 2 Governed by the ability of an unstrengthened building to withstand severe damage or collapse.
- 3 Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges which throw fragments farther than vehicle bombs.

Figure 24.11 A guideline for determining safe distance from an explosive device. (Source: Federal Emergency Management Agency and US Department of Defense, Technical Support Working Group, ISBN: 0-16-061616-6).

The type of bomb, weight and type of explosives used determines the radius of the “Danger Zone” or “Hot Zone”. Figure 24.11 is a guide for determining the safe distance from an explosive device.

Using a Pipe Bomb located outside a building as an example, the Explosive Incident Template below has been annotated to show a Hot Zone of 300 yards (850 ft from Figure 24.11) rounded to closest 100 yards. This is the minimum distance anyone evacuated from the scene or surrounding buildings should be moved to, and also provides the basis for determining which streets require traffic control. The template also shows the Incident Commander the distance responders such as emergency medical and fire should keep back from the device.

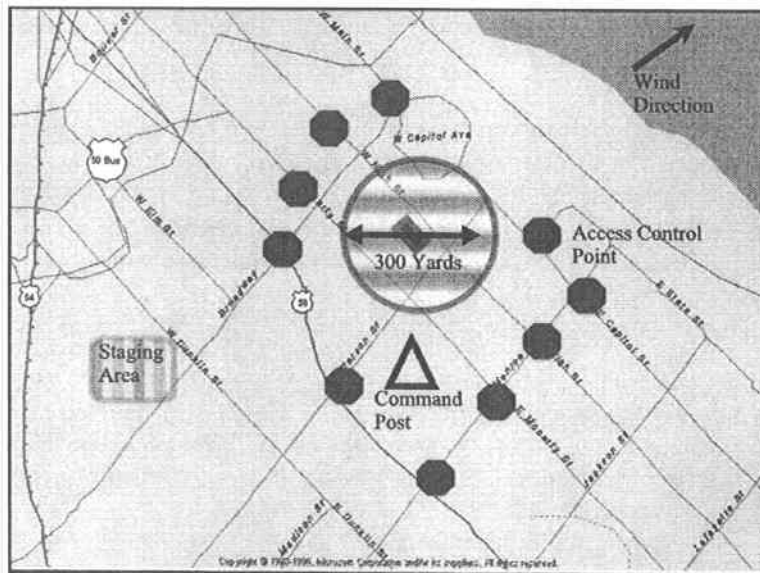


Figure 24.12 Explosive Incident template.

The emergency response priorities for an explosive device incident (no detonation) include:

- Evacuate individuals beyond the Hot Zone.
- Establish security around the scene
- Check for secondary devices, especially in the vicinity of staging and the Command Post.
- Have Fire and Emergency Medical Units report to Staging. A small contingent can be in close proximity to the Hot Zone to facilitate rapid rescue of the Bomb Squad should the device detonate.
- Once all resources are in place, have the Bomb Squad begin assessment, de-arming and removal of the device.

The same template can be used in the event of a device detonation. In this case, the Hot Zone is determined by the location of the furthest away bomb or blast fragment found during a rapid visual search. The Hot Zone size is calculated as that fragment distance multiplied by a factor of 1.5.

Post blast emergency operations require several simultaneous responses. Emergency medical triage and transportation to hospitals for the injured, security of the area, fire suppression, structural evaluation of damaged buildings to determine whether they are safe or pose an immediate hazard to responders and a utility survey to determine the extent of damage and means to provide restoration to unaffected areas. All emergency responders must also be aware of the requirement to limit scene disruption to facilitate evidence collection. The process of evidence collection extends down to the clothing of victims and in many cases the fragments lodged in their bodies.

CHEMICAL INCIDENT RESPONSE TEMPLATE

The response to a chemical incident involving toxic or hazardous materials is driven by several physical and environmental factors. These include:

1. The physical characteristics of the chemical and the way it was disseminated. The vapor pressure of the material will determine how readily it will evaporate. The pH will affect what type of protective clothing (along with toxicity) responders use, type of decontamination required and what detectors will be useful. If the material is atomized or sprayed, it will travel downwind a greater distance than if it is just poured or leaking from a container.
2. The toxicity of the chemical. This will determine what protective equipment is required, type of decontamination system to be used and what antidotes and medical treatments are necessary. It also will determine if residents must be evacuated immediately or if they can be instructed to shelter in place by closing all doors and windows, and shutting off ventilation systems.
3. Environmental factors including time of day, wind speed and direction, temperature and humidity; and terrain contour. The rule for responders is to always stay uphill and upwind from the source of the chemical release. Time of day, temperature and humidity affect rate of evaporation and downwind spread of the material or vapors. Terrain can affect wind patterns, liquid flow patterns and how much material plants and soils may absorb.
4. Types and uses of buildings in the vicinity of the incident. This affects the number of evacuees or contaminated injured caused by the incident. Additional factors are varying air flow patterns around urban

buildings with alters the downwind spreading pattern and the proximity of critical infrastructure such as water systems, communication centers and electrical generating plants.

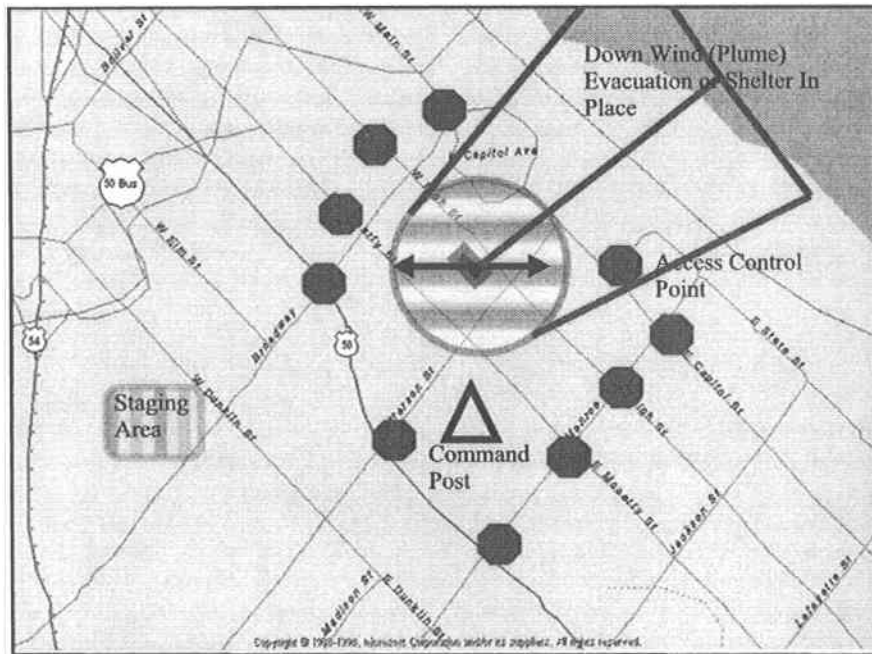


Figure 24.13 Chemical Incident Template.

The Chemical Incident Template reflects an additional “Danger Area” or Hot Zone extending downwind from the point of release along the axis of the wind direction. The initial downwind area is determined using several publications and computer programs such as the “Department of Transportation Emergency Response Guide” or CAMEO, a computer program used by hazardous materials incident responders. More refined computer programs have been developed by the Department of Defense and will likely be used by national responders to an incident.

The initial site and the downwind Hot Zones define the area that may require evacuation or sheltering in place. Due to the increased size of the Hot Zone, additional traffic control points are necessary and the number of affected individuals will be significantly greater.

It is important to note that wind shifts and terrain variances will alter the size and axis of the Hot Zone. The Incident Commander will typically revise the Hot Zone based upon weather forecasts and local observations and information provided by national response organizations and hotlines.

Optimally, the victims and those potentially exposed to the chemical agent will wait for the fire department and emergency medical service to conduct decontamination and triage operations at the scene. Unfortunately this typically is not the case as those victims that are lightly affected will self-refer themselves to hospitals and medical facilities. This increases the potential for contaminating the medical facilities unless a system is in place to rapidly notify all facilities of the incident, and for the facilities to secure all access until additional decontamination teams can be properly dressed in protective clothing and decontamination operations at the medical center initiated. Contaminated individuals allowed into the facility without first going through a decontamination system can have adverse effects on the medical staff thereby reducing the medical capability of the community.

There is a possibility that the number of victims will be greater than the medical capacity of the community. In this case alternate care facilities such as schools or municipal buildings must be designated and activated to relieve the patient burden. Victims with minor or moderate symptoms can be treated in the alternative care centers while the hospitals are used to treat severe cases and those individuals suffering from non-incident medical conditions. Examples of non-incident conditions would include heart attacks, amputations, seizures, etc; the normal cases presented daily to emergency rooms.

Biological Incident Template

A similar template to the Chemical Incident Response Template can be used for a biological agent response with some modifications depending upon the type of agent and the method of delivery used. Typically, a terrorist biological agent attack would be expected inside a building, not outdoors, due to the limited amount of material available. Should the attack take place outdoors, the small size of the individual agent particles will cause them to disperse in a similar manner as atomized liquids. The above assumes that the attack was conducted overtly with warning or was observed by security or other individuals.

The real threat from a biological attack is a successful covert dispersal of material into a crowd. The individuals will not suspect they have been exposed and will not seek treatment immediately. In a few days the initial disease symptoms will appear, but not cause concern as they mimic a cold or the flu. At this point the affected individuals will be dangerously close to being untreatable as the disease has a firm foothold within the body; and may possibly be spreading the disease to family, friends and co-workers. It is conceivable that it might be a week or longer before the disease manifests itself or is detected. This is the crux of the problem with biological weapon attacks.

The first responder's role in a delayed detection event is twofold. First, support as feasible the public health emergency by assisting the public, possibly assisting with treatment centers and drug dissemination centers, and maintaining

security and public safety. Second, the responders must continue to function possibly with reduced staffing levels caused by members also being victims.

The only biological incident or attack that requires direct intervention by first responders is when the means of agent dispersal is the US Mail or other parcel post service. These incidents are usually referred to as suspicious package or letter incidents, and their frequency of occurrence has increased dramatically over the last several years. The September 2001 attack on the World Trade Center and the Pentagon combined with the Anthrax letters in Florida, and Washington, DC caused increased public interest and awareness; and thousands of calls for suspicious item assistance.

It is essential that responders to suspicious package calls do not become complacent due to the high number of hoaxes being observed in the community. Safety and personal protective measures must be employed for each incident. There is also a possibility that the letter does not contain a powder substance but rather an explosive.

The minimum level of protective equipment in these incidents is a light-weight chemical protective suit (Level B), Nitrile Gloves and a full-face respirator with HEPA filter.

In many instances, the presence of a biological agent or explosive can be determined by simply observing the letter or package label and markings. Many of the "Suspicious" packages were actually letters, credit card bills or merchandise the caller forgot ordering. If the item does appear suspicious, and an explosive can be ruled out through observation, then the letter or package should be triple bagged in plastic, the outside washed off with soap and water or a .5% solution of bleach and transported to the nearest diagnostic laboratory for further analysis. The FBI should also be contacted regarding the item, as they may want to open an investigation.

Radiological Incident Template

A radiological incident, short of a nuclear bomb detonation is actually the combination of an explosive mixed with radiological material. Any explosive mixture can be used from complex military and commercial blasting agents to homemade devices. The radiological material can come from a variety of sources including stolen x-ray and other radiograph equipment, highway construction gauges, radiopharmaceuticals or laboratory standards. The intent is to disperse small radioactive particles over a wide area, embedding them in buildings, victims and other items; and to create a downwind hazard area.

Response to this type of incident is similar to both an explosive and a chemical incident. The "Hot Zone" radius is defined by the greater of the distance where the first bomb fragment is found or where the radiation readings first exceed background levels. The plume area is similarly defined as that downrange area where radiation levels exceed background readings. The incident commander may arbitrarily define the downwind danger area based upon environmental fac-

tors, explosive device size (or estimated size) and the levels of radiation observed at the scene.

Responders to a radiological incident must wear protective equipment, which minimizes skin, respiratory, and ingestion pathway exposure. Fortunately, the same equipment used to protect against biological contamination can be used for a radiological event.

Victims and those exposed to the radioactive material must be decontaminated in the same way as those exposed to chemical or biological material. Clothing should be removed, bagged and tagged with their name. Individuals should shower using soap and then dried and monitored for contamination. It is essential that monitoring be conducted after drying to facilitate detection of Alpha radiation, which can be masked by water. An alternative approach that can be used if there is a sufficient number of radiation monitors available is to monitor individuals prior to disrobing, and only having those with elevated radiation readings proceed through the decontamination process. As with other WMD events, urgent medical care should not be delayed until after victim decontamination has occurred.

25

Government and Voluntary Agencies

Julie A. Bentz

*Nuclear Medical Science Officer, National Guard Bureau, Civil Support Office,
Washington D.C.*

INTRODUCTION

The combined emergency management authorities, policies, procedures, and resources of local, state, and Federal governments as well as voluntary disaster relief organizations, the private sector, and international sources constitute a national disaster response framework for providing assistance following a major disaster or emergency. Within this framework, the federal government can provide personnel, equipment, supplies, facilities, and managerial, technical, and advisory services in support of state and local disaster assistance efforts.

The Federal Response Plan (FRP) establishes a process and structure for the systematic, coordinated, and effective delivery of Federal assistance to address the consequences of any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C. 5121, *et seq.*). The FRP sets forth fundamental policies, planning assumptions, a concept of operations, response and recovery actions, and Federal agency responsibilities. The plan describes the array of Federal response, recovery, and mitigation resources available to augment state and local efforts to save lives; protect public health, safety, and property; and aid affected individuals and communities in rebuilding after a disaster. It organizes the types of Federal response assistance that a state is most likely to need under 12 Emergency Support Functions (ESFs), each of which has a designated primary agency. The FRP describes the process and methodology for implementing and managing Federal recovery and mitigation programs and support/technical services and addresses linkages to other Federal emergency operations plans developed for specific incidents. The plan provides a focus for interagency and intergovernmental emergency preparedness, planning,

training, exercising, coordination, and information exchange and serves as the foundation for the development of detailed supplemental plans and procedures to implement Federal response and recovery activities rapidly and efficiently. The FRP covers the full range of complex and constantly changing requirements following a disaster: saving lives, protecting property, and meeting basic human needs (response); restoring the disaster-affected area (recovery); and reducing vulnerability to future disasters (mitigation). The FRP does not specifically address long-term reconstruction and redevelopment.

The FRP applies to all signatory Federal departments and independent agencies that may be tasked to provide assistance in a major disaster or emergency. Additionally, the American Red Cross functions as a Federal agency in coordinating the use of Federal mass care resources in a presidentially declared disaster or emergency. Federal agencies may coordinate with voluntary organizations that provide a wide variety of disaster relief goods and services. Donations often play an important role in supplying disaster victims with essential needs. State and local governments, however, are ultimately in charge of donations, in coordination with national, state, and local voluntary organizations. Federal agencies are encouraged to take advantage of current partnership relations with the private sector. Businesses, both inside and outside the disaster affected area, can supply critical resources during response operations, and assist in restoring essential services and rebuilding the economic base during recovery operations.

The FRP is implemented through regional supplements developed by FEMA and other Federal agency regional offices describing specific actions, operating locations, and relationships to address the unique needs of the region and states within the region. States, along with their local jurisdictions, have their own emergency operations plans describing who will do what, when, and with what resources. In addition, many voluntary, private, and international organizations have emergency or contingency plans.

While the FRP focuses primarily on operational planning specific to an incident, other types of planning also are critical to ensuring effective disaster operations. Pre-incident planning at all levels of government is used to identify operating facilities and resources that might be needed in response and recovery. Action planning, conducted throughout a disaster, establishes priorities with tactical objectives for the next operational period. Contingency planning assists in targeting a specific issue or event arising during the course of a disaster and presents alternative actions to respond to the situation. Strategic planning is used to identify long-term issues such as impact of forecasts and problems such as permanent housing for displaced disaster victims. It also can serve as a blueprint for rebuilding after a disaster.

Under the Stafford Act, a Governor may request the President to declare a major disaster or an emergency if an event is beyond the combined response capabilities of the state and affected local governments. No direct Federal assistance is authorized prior to a Presidential declaration. However, FEMA can use limited pre-declaration authorities to move Initial Response Resources (critical goods

typically needed in the immediate aftermath of a disaster, e.g., food, water, emergency generators) and emergency teams closer to potentially affected areas. FEMA also can activate essential command and control structures to lessen or avert the effects of a disaster and to improve the timeliness of disaster operations. When an incident poses a threat to life and property that cannot be effectively dealt with by the state or local governments, FEMA may request the Department of Defense (DOD) to utilize its resources prior to a declaration to perform any emergency work “essential for the preservation of life and property” under the Stafford Act. Following a declaration, the President may direct any Federal agency to use its authorities and resources in support of state and local assistance efforts to the extent that provision of the support does not conflict with other agency emergency missions.

The FRP also may be implemented in response to the consequences of terrorism, in accordance with Presidential Decision Directive 39 (PDD-39) and PDD-62 that set forth U.S. counterterrorism policy. The FRP Terrorism Incident Annex describes the concept of operations for a unified response to a terrorism incident involving two or more of the following plans: the FRP, the Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Incident Contingency Plan, the Department of Health and Human Services (HHS) Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological Terrorism, the National Contingency Plan (NCP), and the Federal Radiological Emergency Response Plan (FRERP).

LEAD FEDERAL AGENCIES

PDD-39 drew a line in the sand between managing the crisis of a terrorist attack and managing the consequences that result from one. The Department of Justice, through the Federal Bureau of Investigation (FBI), was assigned the lead in the crisis management (CrM) phase. The FBI, therefore, was tasked with anticipating, preventing, or resolving a terrorist incident; dealing with an attack’s immediate aftermath; and carrying out any ensuing criminal investigation. Crisis management is taking measure to identify, acquire, and plan the use of resources needed to anticipate, prevent and/or resolve a threat or act of terrorism. The FBI immediately establishes liaison with the Incident commander. The FBI begins the criminal investigation of the incident immediately, to the extent that it does not interfere with saving lives. The FBI establishes a Joint Operations Center (JOC) to request and integrate all federal assets. Prior to an incident, the FBI provides intelligence to local law enforcement. The lead in the consequence management (CoM) phase was delegated to FEMA. Via the Federal Response Plan, FEMA would oversee the public health and safety angles, as well as the longer term efforts to keep emergency relief flowing and return a community to normalcy as soon and as smoothly as possible. Crisis and consequence management phases can not be separately compartmentalized. They will overlap at the scene of an incident.

In 1998 the White House issued a second terrorism directive, PDD-62, this time focusing solely on weapons of mass destruction. The document, "Protection Against Unconventional Threats to the Homeland and Americans Overseas," reinforced PDD-39's division of labor, but elaborated some federal consequence management duties on the side. PDD-62's more specific terms urged the continuation of first responder training programs through the Defense Department and the provision of equipment to state and local personnel through the Department of Justice. In addition, PDD-62 pegged the Public Health Service under HHS as the lead agency in preparing the medical response to an unconventional terrorist attack and initiated the construction of a national stockpile of antidotes and vaccines. PDD-62 also called for the creation of rapid response teams to help local personnel with chemical and biological weapons terrorism. Finally, PDD-62 carved out a senior-level position on the National Security Council staff—National Coordinator for Security, Infrastructure Protection and Counter-terrorism—to guide and monitor the ever-expanding US counter terrorism effort.

DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION

As attention increasingly focused on weapons of mass destruction and their potential allure for terrorists, the FBI shifted resources and developed new offices to better fulfill its responsibility as lead federal agency for crisis management. The FBI moved first and foremost to augment its intelligence-gathering capabilities related to those plotting or attempting to acquire weapons of mass destruction. In each of its fifty-six field offices, the FBI has appointed a special agent to serve as a focal point for that activity and to aid cities in their coordination with federal assets before and after an attack. These special FBI coordinators have in some cities become catalysts of and a linchpin in local preparedness planning. In numerous cities, the FBI also convenes task forces with sister federal agencies and local law enforcement authorities to promote information sharing about the status of the terrorism threat. The Weapons of Mass Destruction Operations Unit at FBI headquarters directs the federal crisis response to threatened or actual chemical and biological weapons incidents, evaluating threats as they arise and overseeing the resulting criminal investigations. Threats come into the Washington unit from local law enforcement, FBI field offices, the national chemical and biological hotline, or other sources. The FBI then triggers a multi-agency, multidisciplinary team, usually via a telephone conference call, to assess the threat, determine its credibility, and plot the response accordingly. Depending on the threat level, the FBI can then mobilize a number of teams, with specialties in hazardous materials threats, unconventional terrorism, bomb detection, hostage rescue, evidence collection, or negotiation. Of particular utility in these instances is the FBI's Hazardous Materials Response Unit, created to handle criminal investigations of weapons of mass destruction crime scenes. In contrast to other federal response teams that could get involved in rescue or decontamination operation, the HMRU's narrowly

defined mission is to “provide technical, scientific response and forensic support to FBI investigations involving hazardous materials, including weapons of mass destruction.” The HMRU, in other words, enters the picture solely to gather and safely transport forensic evidence on-scene that would support criminal prosecution of the perpetrator(s). The HMRU technically falls within the laboratory division of the FBI and supports FBI field offices contending with hazardous materials and environmental crimes. Based in Quantico, Virginia, the unit comprises just over two dozen personnel on-call twenty-four hours a day to handle anything from requests for technical assistance to rapid deployment to the potential crime scenes. Full teams deploying to the field bring between eight and ten people with a balance of operations experience and scientific background. One unique element of the HMRU is that specialist team members themselves have extensive field experience as firefighters, hazmat technicians, and paramedics, a link that helps build credibility when dealing with their local counterparts in the field.

The two prongs of Justice Department preparedness activity were establishing training and equipment programs. To manage these growing programs, the Attorney General created the Office for State and Local Domestic Preparedness Support within the Office of Justice Programs in 1998. Much of the Justice training efforts take place through a consortium of two federal agencies and three universities each geared to varying specialties and audiences. Courses center on four general areas: basic awareness, responder operations, technician response, and management of a weapons of mass destruction incident. Much of the funds in 2000 flowed to the Center for Domestic Preparedness at Fort McClellan, Alabama. This unique site allows live chemical agent training, which is the focus of the two advanced courses taught there. The realistic training environment has received positive reviews from front-line responders. Pilot courses are also offered through the other four consortium members, covering terrorism awareness for law enforcement, responder operations, and incident command, all with a weapons of mass destruction slant. In addition to consortium training, the Justice Department initiated in 1997 the Metropolitan Firefighter and Emergency Services Program, a two-day basic awareness course geared specifically to firefighters and emergency medical technicians. The Justice Department has taken over responsibility for the Domestic Preparedness Program training courses from the Department of Defense as of October 2000.

The second prong of Justice Department preparedness activity was an equipment grant program. The program’s goal was to provide detection, personal protection, decontamination, and communications equipment to cities that demonstrated need via a description of their current response capabilities, vulnerability to terrorist attacks, and the risk of such an incident occurring. Equipment acquired through the program was specifically earmarked for first responders. Jurisdictions could select from a list of protective, detection, or communication equipment developed by the InterAgency Board for Equipment Standardization and InterOperability. For states to receive equipment through these programs, they must first develop a needs assessment outlining equipment and training requirements with

regard to weapons of mass destruction terrorism. In addition, the Justice Department requires states to craft statewide domestic preparedness strategies covering a three-year period. Packets prepared by the Justice Department walk officials through the process of assessing terrorism risks for communities within their state and offer guidelines for the development of preparedness plans. Block grants went directly to the states, which in turn disbursed the materials to its fire, law enforcement, hazmat, and emergency medical agencies.

FEDERAL EMERGENCY MANAGEMENT AGENCY

Under the Stafford Act, FEMA serves as the primary coordinating agency for consequence management and recovery activities. To carry out this inter-agency role, FEMA executes a wide range of administrative, programmatic, and specialized tasks. Initial tasks include notification, activation, mobilization, deployment, staffing, and facility setup. FEMA processes the Governor's request for disaster assistance, coordinates federal operations under a disaster declaration, and appoints an FCO for each declared state. In continuing operations, FEMA provides support for logistics management; communications and information technology; financial management; community relations, congressional affairs, public information, and other outreach; and information collection, analysis, and dissemination. FEMA is the lead federal agency for all consequence management and disaster relief assistance. When natural disasters sink towns in flood waters or bury them under earthquake rubble, it is FEMA who coordinates the response. Consequence management is predominantly an emergency management function and includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. In an actual or potential terrorist incident, a consequence management response will be managed by FEMA using structures and resources of the Federal Response Plan (FRP). These efforts will include support missions as described in other federal operations plans, such as predictive modeling, protective action recommendations, and mass decontamination. The laws of the United States assign primary authority to the state and local governments to respond to the consequences of terrorism; the federal government provides assistance as required.

In October 1998, the Clinton administration announced the creation of a new interagency office to pull together training and equipment programs and provide local personnel with a link into the federal preparedness network. Dubbed the National Domestic Preparedness Office (NDPO), this new entity was first placed within the FBI and was to help responders and state and local emergency managers identify the programs available to them from an ever-increasing federal list of offerings. NDPO was a single point of contact in Washington for frontline information and federal assistance. To facilitate the coordination, FEMA, HHS, the Department of Defense, and other federal players detailed representatives to

NDPO. The new office grew out of discussions in the summer of 1998 between the Justice Department and stakeholders; state and local officials representing fire, public health, and law enforcement communities. Stakeholders pinpointed six areas where coordination would be beneficial: crisis management planning, training, exercises, equipment, information sharing, and health and medical issues. NDPO's blueprint required the office to identify duplicative areas in federal domestic preparedness training and ensure that it met requisite federal regulatory and industry standards. In May 2001, the Bush Administration moved that part of the coordinated national effort dealing with consequence management out of the FBI and over to FEMA where the Office of National Preparedness was created. The Office coordinates all federal programs dealing with weapons of mass destruction consequence management within the Departments of Defense, Health and Human Services, Justice, and Energy, the Environmental Protection Agency, and other federal agencies. The Office of National Preparedness works with state and local governments to ensure their planning, training, and equipment needs are addressed. FEMA was tasked to work closely with the Department of Justice, in its lead role for crisis management, to ensure a coordinated and cohesive response to the threat from weapons of mass destruction.

DEPARTMENT OF DEFENSE

As directed in PDD-39, the Department of Defense (DOD) will activate technical operations capabilities to support the federal response to threats or acts of WMD terrorism. DOD will coordinate military operations within the United States with the appropriate civilian lead agency(ies) for technical operations. Nuclear, biological and chemical weapons defense has long been part of the military's portfolio. The US Army Institute for Infectious Disease, the US Army Institute for Chemical Defense, the Army's Technical Escort Unit, the National Guard Civil Support Teams and the Naval Medical Research Center are prime examples of pre-existing pockets of military nuclear, biological and chemical defense expertise. Due to its expertise, the US Army was tasked with building a series of training courses for first responders, in coordination with other relevant agencies. In turn, the Army established the Domestic Preparedness Program at Soldier and Biological Chemical Command to develop and execute the training. This Army command also housed another entity that the legislation requested to assist local personnel in chemical and biological weapons incidents, the Chemical and Biological Rapid Response Team.

Nunn-Lugar-Domenici tapped the Pentagon and its chemical and biological weapons expertise from the beginning, reasoning that no one was better prepared to teach the fundamentals of an unfamiliar threat to a lay audience than the experts who know how to defend against it. In restructuring its consequence management architecture, the Pentagon created a unit specifically dedicated to coordinating the military's response to an unconventional attack at home. The Joint Task

Force-Civil Support team integrates domestic unconventional terrorism responses from all the services. Based out of Norfolk, Virginia, at US Joint Forces Command, the new task force is envisioned as the funnel through which all military assistance to first responders would flow in a crisis. The Chemical Biological Rapid Response Team is a joint asset based at Soldier and Biological Chemical Command at Aberdeen, Maryland, that coordinates existing operational specialized military teams capable of addressing particular elements of a chemical and biological weapons crisis. The Army's Technical Escort Unit marries chemical and biological weapons expertise with explosive ordnance disposal capabilities and has more than five decades of varied mission experience. The Technical Escort Unit can bring capabilities in advanced detection, explosive ordnance disposal, decontamination, sampling, and personnel protection. For years, the Technical Escort Unit was virtually the only military unit capable of filling this sort of role—that is, until 1995 when the Marines began to assemble the Chemical and Biological Incident Response Force. The Marines have trained nearly four hundred people for chemical and biological terrorism missions, with expertise in reconnaissance, agent detection and identification, decontamination, security, victim recovery, and casualty treatment. The unit's mission includes force protection as well as consequence management duties. The US Army Medical Research Institute for Infectious Disease (USAMRIID) and the US Army Medical Research Institute for Chemical Defense (USAMRICD) each have biological and chemical technical assets. Based at Fort Detrick in Frederick, Maryland, USAMRIID is the cornerstone of the military's biological defense community, housing expertise in diagnosis, pathology, delivery means, and countermeasures for biological weapons agents. Along with a pool of relevant technical advice, USAMRIID also has an Aeromedical Isolation Team, capable of deploying within twelve hours and transporting two patients in high containment. USAMRICD is located at Aberdeen Proving Ground, Maryland, and represents a parallel center of knowledge about chemical warfare agents, available antidotes, and treatment guidelines. USAMRICD also has a Chemical Casualty Site Team made up of physicians, nurses, toxicologists, and laboratory specialists that is rapidly deployable to give advice on sampling, treatment, and agent identification. Experts from USAMRIID and USAMRICD make up the National Medical Chemical and Biological Advisory Team, a small cell of experts that can deploy within four hours to give first responders specific treatment guidance and decontamination strategies for victims of chemical or biological warfare agents. Given its size, however, this team is an advisory asset, rather than a mass casualty treatment unit. Much like the national team, other short-notice advisory teams are available through Specialized Medical Augmentation Response Teams via the Army's regional medical commands. Focus areas include chemical and biological concerns and preventive medicine, the latter coming from the Center for Health Promotion and Preventive Medicine, also located at Aberdeen Proving Ground. In addition to Army units are the Chemical, Biological, Radiological, Environmental Defense Response Teams from the Naval Environmental and Preventive Medicine Units in Hawaii, California, and Virginia.

The Navy teams are best suited to assist in the remediation process, identifying the lingering environmental hazards after a chemical or biological attack and advising on long-term ways to address any remaining contamination. The Army's 52nd Explosive Ordnance Group have capabilities to render safe a range of sophisticated and improvised explosive devices.

Defense Reform Initiative Directive #25, Presidential Decision Directive 62, and the National Security Strategy of October 1998 directed that the military maintain augmentation forces for weapons of mass destruction (WMD) consequence management, and cited the National Guard as having an important role in this mission area. The National Command Authority has implemented a strategy which leverages the National Guard's ties to the communities throughout the nation, and long-standing tradition of responding to national emergencies, to provide the essential elements and support which the emergency manager requires to manage the potentially catastrophic effects of a WMD emergency. The National Guard's geographic dispersion across the nation reduces the response time, and provides coverage for the majority of the country. The National Guard becomes the lead military element and employs as a state response asset, when called upon by the Governor, to answer the call for assistance. As demonstrated during the many floods, droughts, hurricanes, fires, and the several WMD attacks in the United States, the civil emergency management structure is highly capable of managing large scale catastrophic events. The local and state response forces generally provide a highly capable immediate response, and duration disaster relief. In some cases, however, available resources at the local and state level will require military support, determined by the local and state emergency managers and validated by the Governor of the state or the designated executive agent. When military support is required, the majority of the requests for assistance is performed by the National Guard as a state response asset, under the command and control of the Adjutant General. As a means of assisting the Incident Commander on the ground with the management of a WMD emergency, National Guard Civil Support Teams (CSTs) were fielded to provide the vital bridge between crisis and consequence management, local and state tiers to federal support, and civil to military operations. The CST mission is to support civil authorities at a domestic CBRNE incident site by identifying CBRNE agents/substances, assessing current and projected consequences, advising on response measures and assisting with appropriate requests for state support. The Civil Support Teams provide a full military capability for terrorism response, the ability to determine if a WMD emergency exists, and if so, consult with the Incident Commander (IC) to undertake immediate actions to attempt to control or limit the attack, and subsequently shape the follow-on support.

DEPARTMENT OF ENERGY

The Department of Energy (DOE) has extensive capabilities for radiological accidents/incidents, weapons of mass destruction, and terrorism incidents. DOE gathers, assesses, and shares information on energy system damage and estimations on the impact of energy system outages within affected areas. The suddenness and devastation of a disaster may sever key energy lifelines, constraining supply in affected areas and adversely impacting adjacent areas that have supply links to the directly affected areas. Such an event also could affect transportation, communications, and other lifelines needed for public health and safety. DOE serves as the focal point within the federal government for receipt of reports on damage to energy supply and distribution systems and requirements for system restoration. DOE advises federal, state, and local authorities on priorities for energy restoration, assistance, and supply. DOE assists industry, state, and local emergency response actions and assists federal departments and agencies by locating fuel for transportation, communications, emergency operations, and national defense. DOE has fixed and rotary wing aircraft for aerial radiological surveys and can provide health professionals, monitoring and other expertise. DOE's nuclear emergency search team (NEST) can locate and render safe nuclear or radiological devices. Upon activation DOE Headquarters will establish the Headquarters Emergency Management Team (EMT). DOE Headquarters will assign personnel to temporary duty at the Federal Emergency Management (FEMA) Headquarters, Regional Operations Center, and Disaster Field Office as needed. The priority will be to save lives, protect property, and assist in the restoration of damaged energy systems. As directed in PDD-39, DOE will activate technical operations capabilities to support the federal response to threats or acts of WMD terrorism. In addition, the FBI has concluded formal agreements with DOE as the probable LFA of the Federal Radiological Emergency Response Plan (FRERP) that provide for interface, coordination, and technical assistance in support of the FBI's mission. If the FRERP is implemented concurrently with the FRP the Federal On-Scene Commander under the FRERP will coordinate the FRERP response with the FEMA official who is responsible for coordination of all federal support to state and local governments. The FRERP response may include on-site management, radiological monitoring and assessment, development of federal protective action recommendations, and provision of information on the radiological response to the public, the White House, Members of Congress, and foreign governments. The LFA of the FRERP will serve as the primary federal source of information regarding on-site radiological conditions and off-site radiological effects.

ENVIRONMENTAL PROTECTION AGENCY

As directed in PDD-39, the Environmental Protection Agency (EPA) will activate technical operations capabilities to support the federal response to acts of WMD terrorism. EPA may coordinate with individual agencies identified in the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) to use the structure, relationships, and capabilities of the National Response System as described in the NCP to support response operations. If the NCP is implemented the Hazardous Materials On-Scene Coordinator will coordinate the NCP response with the FEMA official who is responsible for on-scene coordination of all federal support to state and local governments. The NCP response may include threat assessment, consultation, agent identification, hazard detection and reduction, environmental monitoring, decontamination, and long-term site restoration (environmental cleanup) operations. The Environmental Protection Agency (EPA) handles various federal emergency plans for controlling and removing hazardous chemical and oil spills as well as hazardous waste cleanup or investigations. Given the potential utility of hazardous materials management skills in a chemical terror attack, EPA assistance in these areas could contribute to post-incident cleanup efforts. At the top of the EPA's response pyramid is the National Response Center, a hotline staffed twenty-four hours a day by Coast Guard personnel. Calls prompt appropriate interagency coordination through the National Response Team, as well as activation of one or more of the thirteen interagency Regional Response Teams located throughout the United States. These regional teams, which include federal and state personnel, are oriented more toward command and control than on-scene response. From an operational standpoint, cleanup execution comes through a partnership of local personnel, a handful of expert rapid response teams from the EPA and Coast Guard, and the EPA's On-Scene Coordinators who integrate into the unified command structure. The EPA's Environmental Response Team is equipped with monitoring devices to gauge chemical contamination, including chemical warfare agents, and advanced analytical instruments to identify substances and track chemical plumes. Team members are trained to operate in the highest level of protective gear. The Coast Guard can also deploy three operational teams units geared primarily for marine emergencies and public affairs. Like their EPA counterparts, the three Coast Guard strike teams can also carry out their cleanup duties while suited up to the highest levels of personal protection. EPA can provide contractor support. EPA will be key in the long term thorough clean up of the incident site.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

As directed in PDD-39, the Department of Health and Human Services (HHS) will activate technical operations capabilities to support the federal response to threats or acts of WMD terrorism. HHS may coordinate with individual

agencies identified in the HHS Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism, to use the structure, relationships, and capabilities described in the HHS plan to support response operations. If the HHS plan is implemented, the HHS on-scene representative will coordinate the HHS plan response with the FEMA who is responsible for on-scene coordination of all federal support to state and local governments. The HHS plan response may include threat assessment, consultation, agent identification, epidemiological investigation, hazard detection and reduction, decontamination, public health support, medical support, and pharmaceutical support operations. Recently, the HHS has beefed up front-line preparedness by developing local medical response teams geared to offer medical services in the wake of a poison gas or germ attack. The growing involvement of HHS in terrorism preparedness is logical given the agency's established role in the Federal Response Plan for public health issues and its long-time involvement in the National Disaster Medical System. In June 1996, HHS issued a plan on how best to grapple with the unique health and medical consequences of a chemical or biological terrorist incident, including the increased demand for pharmaceuticals, antidotes, and specialized equipment, as well as the narrow window of opportunity to treat victims and counteract the adverse effects of the agents to which they were exposed. Working within the existing crisis and consequence management architecture, the HHS plan committed various agencies to handle key elements of the immediate medical response. Biological agent identification would fall to the Centers for Disease Control and Prevention, as would the epidemiological investigation; pharmaceutical support would come from the Food and Drug Administration; and coordination of mortuary services, transportation and supplies, pathology, and public affairs would fall to the NDMS throughout the HHS Office of Emergency Preparedness.

HHS has articulated its strategy for bioterrorism preparedness centering on five key programming areas: 1) deter or prevent bioterror attacks through tightened shipping controls; 2) upgrade state and local surveillance capabilities; 3) develop better local and national medical and public health responses to bioterrorism; 4) build a national pharmaceutical stockpile; and 5) research additional vaccines and rapid screens for toxic agents. HHS has tried to build local capacity that could manage without federal help during the immediate hours after an attack before meaningful federal help could arrive. HHS terrorism preparedness programs, both federally and locally, are directed primarily by the HHS Office for Emergency Preparedness and the CDC. The main involvement of the Office for Emergency Preparedness comes through contracts with cities to prepare chemical and biological action plans and establish local Metropolitan Medical Response System (MMRS) teams. These teams provide medical resources in the immediate window after a chemical or biological terror attack. To provide specialized medical assistance to other areas, the Office of Emergency Preparedness also designed four National Medical Response Teams to respond to attacks involving weapons of mass destruction. These squads are essentially enhanced Disaster Medical Assistance Teams. Along with personnel and equipment, the teams also possess

enough pharmaceuticals to treat up to five thousand victims of a chemical attack, a cache that can be airborne within four hours. HHS had assigned the Department of Veterans Affairs the task of maintaining the pharmaceutical stock caches, a selection that made sense in light of its experience with managing pharmaceuticals for the Veterans Affairs hospital network. The Centers for Disease Control and Prevention (CDC) has also focused on building capacities at the local, state, and federal levels. Rooted in the US anti-malaria program in World War II, the CDC began in 1946 as the Communicable Disease Center. Since that time, it has served as the primary US brain trust on disease origins, recognition, control, and prevention.

The dozen-odd research centers and offices that fall under the CDC's umbrella cover everything from occupational health to disease research, with several playing an integral role in US preparedness for bioterrorism. The particular advantage of CDC's bioterrorism programs lies in their multiple utility: improvements to the public health infrastructure bring day-to-day benefits regardless of the specific disease or its source and are useful well beyond the worst case bioterrorist scenarios. While CDC carved out an office in the National Center for Infectious Diseases dedicated to bioterrorism preparedness in December 1998, it also set about making widespread improvements to its approach to managing infectious disease. The CDC also began working through state public health agencies to rejuvenate *local* public health infrastructure, creating a layered system of consultation and information sharing among laboratories of varying capacity and specialization. The Laboratory Response Network for Bioterrorism includes four functional levels of laboratories: * Level A: public health and hospital laboratories with minimal biosafety facilities; * Level B: state and county public health agency facilities capable of testing for specific agents and forwarding specimens to higher containment facilities; * Level C: state agencies, academic research or federal laboratories equipped for toxicity testing and advanced diagnostics; * Level D: federal laboratories with highest level of containment and technological sophistication (e.g., CDC, US Army Medical Research Institute for Infectious Diseases). To prevent inundation at the top of the laboratory pyramid, CDC began spreading diagnostic technology down the line to Level B and C laboratories so that they can conduct sample testing. Nevertheless, CDC's rapid response laboratory remains on standby twenty-four hours a day, seven days a week, to confirm local laboratory findings and serve as a reference for questions that pop up in the course of an investigation. In addition to refurbishing the capabilities of state and local labs, CDC has received funding to develop the national pharmaceutical stockpile, ready for immediate deployment to localities caught in a bioterror incident. These supplies are intended for use by local medical personnel within the first twenty-four hours of an outbreak, picking up when local resources are exhausted. The stores consist of key drugs—antibiotics, anti-toxins, and vaccines for a selection of potential biological weapons agents—and medical equipment that would be in high demand, such as ventilators, intravenous fluid kits, and syringes. The stockpile itself is comprised first of "push packages," supplies stored on color-coded pallets at four locations in the United States ready for deployment within twelve hours. The

second stockpile component is vendor-managed inventory, designed to fill in if the initial pallets prove insufficient. This secondary influx consists of goods coming directly from pharmaceutical manufacturers that have contracted with CDC to hold specified amounts of inventory and release it in times of emergency. The Department of Veterans Affairs has been made responsible for procuring and managing the national stockpile contents. The VA will maintain caches of NMC-specific medical supplies and would provide emergency health services to the general public in the event of a WMD incident.

PLANNING ASSUMPTIONS

A major disaster or emergency will cause numerous fatalities and injuries, property loss, and disruption of normal life-support systems, and will have an impact on the regional economic, physical, and social infrastructures. The extent of casualties and damage will reflect factors such as the time of occurrence, severity of impact, weather conditions, population density, building construction, and the possible triggering of secondary events such as fires and floods. The large number of casualties, heavy damage to buildings and basic infrastructure, and disruption of essential public services will overwhelm the capabilities of the state and its local governments to meet the needs of the situation, and the President will declare a major disaster or emergency. federal agencies will need to respond on short notice to provide timely and effective assistance. The degree of federal involvement will be related to the severity and magnitude of the event as well as the state and local need for external support. The most devastating disasters may require the full range of federal response and recovery assistance. Less damaging disasters may require only partial federal response and recovery assistance. Some disasters may require only federal recovery assistance.

CONCEPT OF OPERATIONS

Most disasters and emergencies are handled by local and state responders. The federal government is called upon to provide supplemental assistance when the consequences of a disaster exceed local and state capabilities. If needed, the federal government can mobilize an array of resources to support state and local efforts. Various emergency teams, support personnel, specialized equipment, operating facilities, assistance programs, and access to private-sector resources constitute the overall federal disaster operations system. The FRP describes the major components of the system, as well as the structure for coordinating federal response and recovery actions necessary to address state-identified requirements and priorities.

The FRP employs a multiagency operational structure that uses the principles of the Incident Command System (ICS), based on a model adopted by the fire and rescue community. ICS can be used in any size or type of disaster to control

response personnel, facilities, and equipment. ICS principles include use of common terminology, modular organization, integrated communications, unified command structure, action planning, manageable span-of-control, pre-designated facilities, and comprehensive resource management. The basic functional modules of ICS (e.g., operations, logistics) can be expanded or contracted to meet requirements as an event progresses. Consistent with ICS principles, the FRP can be partially or fully implemented, in anticipation of a significant event or in response to an actual event. Selective implementation through the activation of one or more of the system's components allows maximum flexibility in meeting the unique operational requirements of the situation and interacting with differing state systems and capabilities.

An incident involving hazardous substances, weapons of mass destruction, or other lethal agents or materials may require a response under another federal emergency operations plan (National Contingency Plan, Federal Radiological Emergency Response Plan, etc.). These plans delineate measures necessary to handle or contain released materials and keep the public properly informed and protected.

INTEGRATION OF RESPONSE, RECOVERY & MITIGATION ACTIONS

Following a disaster, immediate response operations to save lives, protect property, and meet basic human needs have precedence over recovery and mitigation. However, initial recovery planning should commence at once in tandem with response operations. Actual recovery operations will be initiated commensurate with state priorities and based on availability of resources immediately required for response operations. In recognition that certain response and recovery activities may be conducted concurrently, coordination at all levels is essential to ensure consistent federal actions throughout the disaster. Mitigation opportunities should be actively considered throughout disaster operations. Decisions made during response and recovery operations can either enhance or hinder subsequent mitigation activities. The urgency to rebuild as soon as possible must be weighed against the longer term goal of reducing future risk and lessening possible impacts should another disaster occur.

MILITARY SUPPORT

DOD maintains significant resources (personnel, equipment, and supplies) that may be available to support the federal response to a major disaster or emergency. DOD will normally provide support only when other resources are unavailable, and only if such support does not interfere with its primary mission or ability to respond to operational contingencies.

National-level requests for military support are made through the Director of Military Support (DOMS), who represents the DOD for provision of military as-

sistance to civil authorities. DOMS exercises national-level oversight of the Defense Coordinating Officer (DCO) function.

Requests for military support at the Disaster Field Office (DFO) are processed through the DCO, the military official specifically designated to orchestrate DOD support. To ensure a coordinated and consistent DOD disaster response, the DCO is the single point of contact in the field for coordinating and validating the use of DOD resources (excluding those provided by the U.S. Army Corps of Engineers (USACE) when operating as the primary agency for ESF #3 — Public Works and Engineering, and those of the National Guard forces operating under state control). The DCO is the designated DOD on-scene member of the ERT and coordinates RFAs and mission assignments with the FCO. The DCO is supported on scene by a Defense Coordinating Element (DCE), composed of administrative staff and liaison personnel, including the Emergency Preparedness Liaison Officer (EPLO), who normally will collocate with the ERT Operations Section. Specific responsibilities of the DCO include validating requirements for military support (i.e., determining if the military could and should support the request); forwarding mission assignments to the appropriate military organization(s); and assigning military liaison officers to provide technical assistance to applicable activated ESFs. The DCO, through appropriate military channels, refers problematic/contentious military support issues to DOMS. DOMS facilitates resolution of issues at the national level.

Based on the magnitude and type of disaster and the anticipated level of resource involvement, DOD may establish a Joint Task Force (JTF) or Response Task Force (RTF) to consolidate and manage supporting operational military activities. Both task forces are temporary, multiservice organizations created to provide a consequence management response to a major natural or man-made disaster or emergency. The JTF responds to major disasters such as hurricanes or floods. The RTF responds to events involving the use, or possible use, of chemical, biological, and/or highly explosive agents/materials. A JTF or RTF commander exercises operational control of all allocated DOD assets (except USACE personnel executing ESF #3 missions and the Joint Special Operations Task Force); provides personnel, equipment, and supplies to the affected area; and provides disaster response support based on mission assignments received through the DCO. Although both commanders may supplant the DCO as the senior DOD representative, the DCO will continue to exercise the ERT staff function of mission assignment coordination and validation, and will act as a liaison between the ERT staff and the JTF or RTF staff.

FEDERAL LAW ENFORCEMENT ASSISTANCE

In a disaster or emergency, each state has primary responsibility for law enforcement, using state and local resources, including the National Guard (to the extent that the National Guard remains under state authority and has not been

called into federal service or ordered to active duty). Accordingly, the FRP makes no provision for direct federal support of law enforcement functions in a disaster or emergency.

If a state government should experience a law enforcement emergency (including one in connection with a disaster or emergency) in which it could not provide an adequate response to protect the lives and property of citizens, the state (on behalf of itself or a local unit of government) might submit an application in writing from the Governor to the Attorney General of the United States to request emergency federal law enforcement assistance under the Justice Assistance Act of 1984 (42 U.S.C. 10501-10513) as prescribed in 28 CFR 65. The Attorney General will approve or disapprove the application no later than 10 days after receipt. If the application is approved, federal law enforcement assistance may be provided to include equipment, training, intelligence, and personnel.

In the event that state and local police forces (including the National Guard operating under state control) are unable to adequately respond to a civil disturbance or other serious law enforcement emergency, a Governor may request, through the Attorney General, federal military assistance under 10 U.S.C. 15. Pursuant to 10 U.S.C. 331-333, the President will ultimately determine whether to use the Armed Forces to respond to a law enforcement emergency. Under Title 10 authority, the President may federalize and deploy all or part of any state's National Guard.

RESPONSE AND RECOVERY ACTIONS

Federal agencies are prepared to take a variety of actions to assist state and local governments in responding to and recovering from a major disaster. These actions range from initial notification of a disaster to preparation of a final disaster after-action report. They are not necessarily in sequential order; some may be undertaken concurrently. An overview of an entire disaster operation, indicating key operational components and the typical sequence of actions, appears at the end of Chapter 23.

INITIAL ACTIONS

Upon indication of an imminent or actual disaster, the state notifies the FEMA Regional Office through the MERS Operations Center 800 number. The MOC then immediately notifies the NECC and FEMA regional staff in accordance with regional procedures. If directed by the Regional Director, the MOC also notifies regional agency representatives. The NECC notifies key FEMA headquarters staff and other federal agencies through their respective agency EOCs and/or designated individual(s). An Advisory is issued to provide an early warning that a possible event being monitored may result in activation. The Advisory is for information only and requires no formal action. An Alert is issued when

an imminent or actual event is likely to result in activation. It puts federal responders on notice that they need to be ready for immediate deployment. An Activation directs immediate deployment to the location specified in the notice. A Cancellation indicates that no further action is required or that an activation notification is being terminated. CDRG members may be notified to convene at FEMA Headquarters for an initial meeting, depending on the nature of the disaster. CDRG members or alternates remain on call to meet at any time during the disaster response.

The FEMA Regional Director deploys a FEMA state Liaison to the state EOC to provide advice on the declaration process and available federal assistance, and also partially or fully activates the ROC staff, including regional agency representatives. With the support of ESFs, the ROC staff initially deploys members of the ERT-A, including damage assessment personnel, to state operating facilities and disaster sites to assess the impact of the situation, collect damage information, and determine requirements. If regional resources appear to be overwhelmed or in an event having potentially significant consequences, FEMA Headquarters may deploy an ERT-N to coordinate the initial response. Meanwhile, if directed by FEMA Headquarters, the NECC informs ESF primary agencies of an EST activation and provides a time for each activated ESF to report to FEMA Headquarters, as part of the EST. Primary agencies are responsible for activation of their support agencies if required. Agencies may activate their headquarters EOCs to provide coordination and direction to their regional response elements in the field. The Regional Director processes the Governor's request for a Presidential declaration, which indicates the extent of damage and the types of federal assistance required. FEMA Headquarters then forwards the Governor's request to the White House, along with a recommended course of action. Concurrent with a Presidential declaration of a major disaster or emergency and official appointment of an FCO, FEMA designates the types of assistance to be made available and the counties eligible to receive assistance. The Regional Director appoints a Disaster Recovery Manager. The ROC and EST Logistics Section support the establishment of a DFO and mobilization center(s). The ROC also coordinates federal support of state requirements until the FCO assumes those responsibilities. A Joint Information Center (JIC) may be established, as required, to provide a central point for coordinating emergency public information activities. The ERT-A/ERT-N coordinates damage assessment and selection of locations for field facilities with the state. It also coordinates mission assignments for direct federal assistance and procurement of goods and services with the Comptroller and ROC staff. The ERT-A/ERT-N begins the transition to a partial or full ERT. ESFs act quickly to determine the impact of a disaster on their own capabilities and to identify, mobilize, and deploy resources to support response activities in the affected state. The EST begins interagency operations by supporting initial activation, mission assignment requirements, and ROC staff activities as needed.

CONTINUING ACTIONS

The ERT-A/ERT-N completes the transition to a full ERT by the addition of staff, including ESF representatives. Headed by the FCO and located at the DFO, the ERT assumes operational responsibility from the ROC staff for coordinating federal disaster assistance in support of state-identified needs and priorities submitted by the SCO. The ESF representatives on the ERT coordinate federal assistance under their respective ESF missions. To the extent possible, they maintain contact with their state counterparts. At FEMA Headquarters, the EST provides financial, administrative, logistical, and operational support to the ERT and ROC as required, including coordinating the deployment of emergency teams and supplies. The CDRG convenes as needed to address policy issues such as allocation of scarce federal resources. Early in the response, the Deputy FCO for Mitigation plays a critical role in identifying mitigation opportunities and educating disaster workers on the merits of incorporating mitigation measures into response and recovery actions. Congressional affairs staff from FEMA and supporting agencies conduct briefings for Members of Congress and staff as appropriate. Working with other federal and state environmental agencies, the Environmental Officer identifies environmental and historic resources that might require consideration under the law as response and recovery efforts are implemented. Once immediate response missions and lifesaving activities conclude, emergency teams are demobilized and the emphasis shifts from response to recovery operations. The ERT Information and Planning Section develops a demobilization plan for the ERT during response operations.

The ERT Operations Section is the central coordination point among state and federal agencies and voluntary organizations for delivering recovery assistance programs. The Human Services and Infrastructure Support Branches of the Operations Section assess state and local recovery needs at the outset of the disaster and relevant time frames for program delivery. The branches ensure that federal agencies that might have appropriate recovery assistance programs are notified of the disaster and share relevant applicant and damage information with all involved agencies. In conjunction with the SCO, the FCO determines the need for DRCs in the disaster area. State and federal agencies staff the DRCs with knowledgeable officials who provide recovery program information, advice, counseling, and technical assistance related to mitigation. The Human Services Branch of the ERT coordinates assistance programs to help individuals, families, and businesses meet basic needs and return to self-sufficiency. The branch also coordinates with voluntary organizations and may become involved in donations management. The Infrastructure Support Branch of the ERT coordinates assistance programs to aid state and local governments and eligible private nonprofit organizations to repair or replace damaged public facilities. The two branches assist in identifying appropriate agency assistance programs to meet applicant needs, synchronizing assistance delivery, and encouraging incorporation of mitigation measures where possible. Additionally, they track overall progress of the recovery effort, particularly

noting potential program deficiencies and problem areas. The Deputy FCO for Mitigation coordinates agency assessment of mitigation program needs and begins to match federal and state resources to meet those needs.

When a centralized federal coordination presence is no longer required in the affected area, the ERT implements the demobilization plan to transfer responsibilities and close out the DFO. Recovery assistance program oversight and monitoring then shifts back to individual agencies' regional offices or headquarters.

Following a disaster, the FCO submits an after-action report through the ERT Information and Planning Section to FEMA Headquarters detailing problems encountered and key issues affecting federal performance. Data from these issues and targeted reviews are analyzed and provided to appropriate FEMA management for consideration. After a particularly large or unique disaster operation, FEMA also may convene an interagency forum to identify lessons learned. Each federal agency involved is encouraged to keep records of its activity to assist in preparing its own after-action report.

BIBLIOGRAPHY

FBI WMD Incident Contingency Plan.

Federal Response Plan, <http://www.fema.gov/r-n-r/frp/>, accessed 5/2002

Federal Radiological Emergency Response Plan, <http://www.fema.gov/pte/rep/350-5.htm>, accessed 5/2002

HHS Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological Terrorism.

National Contingency Plan, <http://www.fema.gov/r-n-r/frp/frpintro.htm>, accessed 5/2002

Presidential Decision Directive 39, U.S. Policy on Counterterrorism. An unclassified extract may be obtained from FEMA.

PDD-39, Domestic Deployment Guidelines.

PDD-62, Protection Against Unconventional Threats to the Homeland and Americans Overseas.

26

Bioterrorism: Consequences and Medical Preparedness

L. David Ormerod

University of Missouri, Columbia, Missouri

INTRODUCTION

On December 9, 2002, 20 cases of smallpox are confirmed in Oklahoma and additional cases are suspected in Georgia and Pennsylvania (Fictitious cases) [1]. As smallpox virus was eradicated in 1980, except for two high-security scientific laboratories, it is presumed that a bioterrorist attack has almost certainly occurred, but from where - an international source or domestic? The National Security Council (NSC) meets to plan strategy. Containment must primarily be by vaccination as there are no useful therapeutic agents, but there are only 12M doses of smallpox vaccine stockpiled. Among the most immediate decisions to be made are to determine who to vaccinate, where, and how. It is known that smallpox is highly infectious and it is anticipated that one-third of patients will die. What do you tell the public?

By December 15, 2002, there are 2,000 cases in 15 states and isolated cases in Canada, Mexico, and the United Kingdom. The local medical facilities in affected areas are overwhelmed, vaccine supplies are dwindling, and social unrest is increasing rapidly. Federal and some state borders are closed, and commerce is disrupted. With the failure of initial containment, how are the local, state, and federal authorities to respond to this worsening situation?

The epidemic continues to deteriorate. A week later on December 22, 2002, there are now 16,000 cases in 25 states and 1,000 deaths, and 10 foreign countries are involved. The most cogent prediction is that within another 3 weeks 300,000 people will become infected by smallpox and 100,000 will ultimately die. Vaccine supplies are depleted. There is uncertainty as to whether new cases of infection are

being acquired from known infected individuals, from unvaccinated contacts, as a result of ineffective vaccine, or from new bioterrorist attacks. The national economy is badly affected. Food supplies are scarce, populations increasingly desperate, and the affected states have restricted all nonessential travel. The source of the attack is still unknown. How should the federal government respond?

Although of low probability, this scenario is certainly feasible [2, 3]. It was presented in June 2001 as a major exercise in defense preparedness at Andrews Air Force Base, Washington DC, entitled "Dark Winter." Former senior government officials, senior administrators with policy or operational responsibilities in biological weapon preparedness, and experienced journalists were involved in a 2-day planning exercise constructed as a series of mock NSC meetings. Among the study conclusions were that: (1) US government leadership is unfamiliar with the consequences and policy options pursuant to major biological weapon (BW) attack; (2) the potential constitutional conflicts that may exist between state and federal interests in a situation with limiting options were not foreseen; (3) there was incomplete recognition of the centrality of public health and medical expertise in what might be a prolonged emergency, and this allied to poor preparedness; (4) there is a critical lack of surge capacity in the US health system; and (5) the rapid dissemination of accurate information, untainted by political constraints, is of paramount importance in bioterrorism (BT) because of the potential for social dislocation.

It has first to be recognized that the response to BT is fundamentally different from the response to other kinds of terrorism. After BW attack, the medical community is the front line. The Federal Response Plan (FRP) apparatus of crisis and consequence disaster management with its emphasis on mass disaster scene rescue capabilities will characteristically not be involved primarily, as there will likely be no disaster scene in its conventional meaning.

For a century, civilian and military public health officials have been entrusted with the management of public health crises. The unwieldy FRP structure that has been devised to respond to disaster management including terrorism (see Figure 10.2), inserts a bureaucracy, experienced in the coordinated fire services-hazardous materials (HAZMAT)-emergency medical services-law enforcement dialectic, into epidemic control [4]. In a prolonged medical emergency, the assets of the FRP will be critical, but the decision-making and coordination would probably be better placed in experienced medical hands trained in disaster management and supported in the FRP hierarchy. It is not yet clear what new directions will result from the recently formed Office of Homeland Security (OHS).

Disaster management under the FRP is divided into (A) crisis management under the leadership of the Department of Justice (DOJ) in the guise of the Federal Bureau of Investigation (FBI), and (B) consequence management under the leadership of the Federal Emergency Management Agency (FEMA) and the FEMA Office of National Preparedness (ONP). The Department of Health and Social Security (DHSS) is the primary agency for Health and Medical Services pursuant to the FRP Emergency Support Function (ESF) #8. Considerable planning and

preparedness development is being fostered through its lead agency, the Centers for Disease Control and Prevention (CDC), the CDC Bioterrorism Preparedness Response Program (BPRP), and the HHS Office of Emergency Preparedness (HHS/OEP). As a result of the Nunn-Lugar-Domenici Act (1997), there has been extensive educational activity in biodefense preparedness training formulated by numerous federal sources, including HHS [5,6], FEMA [7], the Department of Defense (DOD) [8], other agencies[9] and non-governmental organizations (NGOs) [10]. Many of these programs were replicative and often failed to reach their target audience [11].

EPIDEMIOLOGY OF BIOTERRORISM

The nature of terrorism predicates that no government can reduce the risk to which its population is subject to zero, no matter the magnitude of the investment. Although the dangers of bioterrorism have been recognized by the defense community for many years, until recently the strategic risks were believed small, confined by technical and tactical difficulties, and by the moral opprobrium associated with the deliberate, uncontrolled release of epidemic diseases into the civilian community. Responsible science was also reluctant to invite the problem. As Henderson has said, "until recently, I had doubts about publicizing the subject because of concern that it might entice some to undertake dangerous, perhaps catastrophic experiments. However, events have made it clear that likely perpetrators already envisage every possible scenario" [12]. What is the present risk of bioterrorism in the US?

The question has recently been explored in detail [13-16]. In the early 1970s, more than 100 countries including the United States ratified the Biological and Toxin Weapons Convention (1972). The US BW Program was terminated in 1969/1970 and the US stockpile of biological weapons destroyed [17]. Although most nations complied, a few, notably the former Soviet Union, Iraq, North Korea, Israel, and South Africa, continued to develop BW, and most remain potential sources of 'weapons-grade' infective agents for international and national terrorist groups. The development of BW requires little specialized equipment and information on the science and technology is openly available. The professional skills can be hired and the processes are indeed generally inexpensive. However, there remain key technical problems that have to be overcome to produce an effective BW, notably the dangers of contamination, considerations of scaling-up bench-top production methodology, technicalities in microbial biology, and difficulties in establishing an effective delivery system-usually some form of aerosolization (Chapter 4). Governments have found it necessary to employ hundreds of scientists to weaponize BW (Chapter 6) as weapons of mass destruction (WMD). The assumption that BW are potentially easy to develop is an over-simplification. Unless a terrorist group is technologically sophisticated, the most likely means for terrorists to obtain BW WMD is to steal or purchase them on the black market.

The Aum Shinrikyo terrorist attacks on Matsumoto (1994) and the Tokyo subway (1995) using sarin gas overshadowed the cult's failure to weaponize and disseminate anthrax and botulinum successfully. However, this development of a potential urban capability in bioterrorism generated shockwaves throughout the US defense community, already alerted by the concomitant danger of dissemination of insecure BW stockpiles in the former Soviet Union [18], and by the disclosure of Iraq's BW capability [18] and its use of chemical weapons in Kurdistan.

The historical record demonstrates only a small but significant terrorist use of biological agents, and almost invariably with unsophisticated weapons. The gradual increase in the number and severity of conventional terrorist attacks and the predilection for more indiscriminate targeting associated with groups motivated by religion, religious cults, and Christian far right groups, when contrasted with politically motivated groups, has been interpreted to represent an increased risk to the US population [19]. However, although members from across the spectrum of terrorist groups have attempted to acquire BW, very few groups have undertaken long-term programs to develop and use them. There is no credible indication, for example, that Osama bin Laden's network has obtained BW. For strategic reasons, most terrorist groups indeed operate well below their individual capacity for violence. The Deputy Assistant Director for Counterterrorism testified in July 2000, "Currently, there is no credible intelligence that a terrorist group has acquired, developed, or is planning to use chemical, biological, or radiological agents in the United States" [20]. The recent US anthrax attacks are believed to have a domestic origin and a research laboratory source is suspected.

The current obstacles to volume production, weaponizing, and dissemination of hazardous infective agents or toxins is likely to change over time, however, as scientific knowledge disseminates and technology becomes more readily available. At present, terrorist attempts to develop BW are likely to produce agents with limited infectivity, restricted to use as an environmental contaminant indoors. Initial target population exposures would be relatively small. Use of a highly contagious agent as a contaminant could possibly still generate a large epidemic should the BW attack go undetected and containment measures not taken. For example, a single undiagnosed case of smallpox that was imported into the former Yugoslavia in 1972 resulted in 175 cases and 35 deaths. Ten thousand contacts were quarantined in hotels guarded by the military and the entire nation of 20 million people was vaccinated [21] Even low technology microevents therefore have the potential for producing disease, disability, and death, civil and social unrest, and economic disruption.

It is the fully weaponized and optimized BW (Chapter 6) and its skilled dissemination utilizing knowledge of meteorological and microclimatic conditions, or of building or vessel ventilation systems, that gives BW the potential for use as weapons of mass destruction. Some biological attacks could have greater potential for loss of life than a nuclear device. It is this feasible doomsday scenario that has engaged the strategic defense community to recommend the drastic enhancement of homeland security against BW attack. The uniquely inhuman and random na-

ture of an epidemic attack on civilians has profound implications for the security, commerce, and welfare of that society. Even a limited attack would be associated with a heightened moral repugnance. A disseminated BT attack as a "continuation of politics by other means" is quintessentially terrifying and unimaginable to populations long complacent from the public health control of epidemic disease.

At least for the time being, technological constraints suggest that lower-level BT threats will continue to be the most feasible scenario for US homeland security. Biological weapons of mass destruction could be developed by a disciplined terrorist group that could attract biologists and engineers of sufficient caliber and then develop secure larger-scale production capabilities. That conventional explosive and chemical terrorism are less complicated options will tend to counter this risk. Weaponized biological agents might still be obtained from one of the nation states that retain BW stockpiles, but there is no evidence that dissemination of weapons-grade BW from these so-called rogue states has occurred, although thefts of stock cultures have been reported [22]. The strategic risks of discovery to those countries is a deterrent, for the international military response would be formidable.

An aspect that is often neglected in discussions of the relative risks of BT attack is consideration of the strategic and tactical motivations of terrorist groups. It is argued that there is an ineluctable spiral of terrorism lethality [23] that might lead to proliferation of BW use [24]. Whether BW would further terrorist objectives is primarily dependent upon the consequences of their use. This, of course, will vary with the infectious agent used and the technological sophistication of its preparation and dispersion. Terrorist groups generally seek specific political, religious, or social objectives and employ violence to coerce governments to accede to these agendas. In most cases, the goals of terrorism are to generate propaganda and to generate impelling political pressure on their opponents. Extortion, economic dislocation, and political polarization are additional motivations. Violence is typically directed against targets of symbolic value to the nation state.

Although tactics and strategy may change over time, the leadership of most predominantly secular terrorist groups are deterred by the inherent uncontrollability of hazardous biological agents and the sheer magnitude of the casualties that could result. Epidemics fail to respect ethnic, social, and national boundaries. The public alienation and unprecedented international retaliation would almost invariably be counterproductive [19, 25], with the exception perhaps of their limited use against 'legitimate' targets, such as in assassinations or attacks on specific buildings via their air conditioning systems, through agroterrorism (Chapter 8) or through the limited contamination of the food supply—both latter targets are primarily undertaken for their economic consequences. Biological weapons remain a potent intimidatory threat, but to be truly effective, capability for their use does need to be established.

There remains a hard core of militant, religiously motivated terrorist groups with authoritarian decision-making structures that may be without such constraints. Their goals are to undermine the foundations of the State, disengage from

the secular Western World, and restore a fundamentalist culture based upon ancient text. Fervid religious belief can provide the moral imperative for indiscriminate terrorism unencumbered by secular conscience—the heady mix fostered by economic and political impoverishment. Religious cults, such as Aum Shinrikyo, and domestic Christian right wing or apocalyptic groups that purvey a seditious brew of paranoid, volatile, often racist rhetoric also have a predilection for indiscriminate violence. Domestic loner, "loony" terrorists, such as the Unabomber, Ted Kaczinski, can pose a serious threat too.

UTILITY OF BIOLOGICAL WEAPONS

Disparate scenarios must be considered. Lack of an effective BW dispersal mechanism (Chapter 6) will force terrorists to use infectious biological agents as a contaminant in confined spaces. However, to maximize casualties the agent needs to be milled and then aerosolized at a stable particle size of 1-5 μ and dispersed downwind under optimal climatic conditions as a continuous release across a front. In addition, the BW has to be released at sufficient altitude to spread over but not pass over the target. Given the right weather conditions, BW aerosol may drift for up to a hundred miles and have the capacity to infect the inhabitants of a city in its path. At the higher end of the unsophisticated weapon spectrum, fatalities in the low tens of thousands are feasible, whilst a more advanced biological weapon could injure hundreds of thousands [15]. The stability of the BW varies considerably with the infectious agent. Anthrax, for example, is quite robust, but viruses tend to be sensitive to such factors as humidity, desiccation, oxidation, air pollution, ultraviolet light, and excessive heat. Rain will scour an aerosol cloud. BWs are not an all-weather option.

Biological attacks on the nation state may be designed to attain certain objectives: (1) assassination of prominent citizens; (2) indiscriminate targeting of the civilian population; (3) economic and commercial disruption; (4) attack on military facilities; (5) propaganda; and (6) intimidation and blackmail. Aerosol attacks are the most likely option, but BW can also be used to contaminate agricultural animals and crops (Chapter 8), the food industry, and water supplies.

NATURE OF A BIOLOGICAL ATTACK

Most BWs cause diseases that already exist in nature and may occur spontaneously in the US or elsewhere in man and sometimes in animals. With the exception of diseases produced by certain biological toxins in which the effects can be similar to chemical releases, the onset of infection is delayed for a few days with most agents, but for up to several weeks with certain others—a variable interval known as the incubation period. As the infectious agents themselves are usually odorless and colorless and a well produced aerosol is invisible, it may be the exception for the crime scene to be detected contemporaneously. The initial infec-

tious onslaught will likely be an occult event and there will be no opportunity to ameliorate the consequences of the attack until the subsequent epidemic is detected. The perpetrators may have long fled. Crisis management in a BT context may therefore be very different compared to other terrorist attacks.

Several clinical patterns of disease presentation (Chapter 5) are possible depending upon the microbial agent utilized, the size of the inoculum, mode of infection, and the specific immune status of the individual. Aerosol infection is not the usual natural mode of transmission for several of the candidate organisms and this may result in unusual presentations. There are few clinical features specific to these diseases, at least initially. The nature of these often exotic infections can easily be lost among the many conventional diseases presenting in ill individuals with fever, malaise, respiratory, gastrointestinal, or neurological complaints. In particular, the early symptoms may be confused with influenza. Patients are likely to be widely scattered geographically, even internationally.

The front line of BT is the health service. Physicians and other health-care workers are the "first responders". Bioterrorist attacks in the US will usually be first detected by emergency department physicians and nurses, infectious disease consultants, microbiologists in the hospital or regional reference laboratory, hospital infection control officers, county medical examiners, or by specialists in the public health services. To date, however, medicine has been woefully unprepared for such an eventuality. With most contagious BWs, there will only be a short window of opportunity before secondary transmission of infection results in further waves of medical casualties. Avoidable delays in diagnosis, treatment, and vaccination containment may have appalling consequences.

One indicator of BT outdoors may be the concomitant involvement of farm and domestic animals by a number of candidate infectious agents. The use of unexpected agents, the possibility of multiple, separate BW attacks, or an attack using more than one organism need to be considered. It will often not be clear in the initial stages of a terrorist-introduced epidemic whether an outbreak has a natural or a man-made cause. Intelligence reports and/or terrorist claims may be helpful. Considerable public health, epidemiological, and federal resources may be necessary to make this distinction. However, there are a number of features that may be significant in indicating an intentional causation, although none alone are conclusive [26-28].

- (i) Larger epidemics than anticipated, clustering of patients, or with an unusual epidemic pattern
- (ii) Increased numbers of unexplained febrile illness or death, especially if rapidly fatal
- (iii) Unusual age distribution, geographic occurrence, or seasonal onset
- (iv) Much greater or lower rates of infection from certain areas
- (v) Epidemiological findings that suggest a common factor such as location, building, subway, or vessel
- (vi) Single case of disease by exotic agent, e.g., smallpox

- (vii) Concomitant epidemic and zoonotic (in animals) outbreaks
- (viii) Unusual strains, variants, or antibiotic resistance patterns
- (ix) Separate, noncontiguous outbreaks
- (x) Simultaneous epidemics with different organisms

As long as the risk of BT can be confined to local acts of contamination, such as the 2001 US anthrax mail attacks, the current public health and FRP capabilities might be sufficient. However, it is clear to anyone who has visited a US emergency room that a sudden surge of ill patients will rapidly outstrip available capacity. Annual influenza epidemics are handled with difficulty. Add into the equation the contamination of the facilities that may occur, the hazards to unvaccinated staff, and the risk of subsequent waves of infection, and it is clear that nationwide contingency planning must be in place to boost infrastructure and to anticipate all possible eventualities [29, 30].

During a virulent epidemic, emergency rooms, inpatient facilities, isolation rooms, intensive care and respiratory ventilation facilities, laboratories, pharmaceutical supplies, and morgue facilities may be rapidly overwhelmed. Staff may be infected or stay at home-75% of hospital workers are female and in the modern era many are heads of families. Hospitals and essential services might also be primarily incapacitated in the initial attack or subsequently, the local economy and school systems may cease to function, the anxious well may swamp any functioning medical service, and civil panic might complicate disaster management. Albert Camus' "The Plague" [31] and José Saramago's "Blindness" [32] bear eloquent testimony to such events.

The expertise to detect and control an epidemic are primarily provided by medical and public health assets, supplemented and coordinated by local government and by state and federal resources. In recognition of the national vulnerability, considerable enhancements of BT response programs at all levels have been under way since President Clinton's 1995 Presidential Decision Directive, PDD 39. New ways of delivering emergency care and treating patients in temporary facilities may be needed, and arrangements developed for home therapy of the lesser ill and the recuperating. The medical and public health facilities must be strengthened to be able to facilitate the management of unfamiliar epidemics and to accommodate surge capacities. There will be considerable national benefits to accrue from improved disease surveillance, and increased research into diagnosis and management of epidemic infectious disease whether caused by BW candidate agents or by naturally occurring epidemics [33]. It has, however, to be admitted that not all government expenditures in the US Bioterrorism Program have been well advised [11, 34, 35].

The risk of naturally occurring epidemic disease is still ever present. More than 30 previously unknown infectious diseases have been identified since the early 1970s [36], including:

1999	Nipah virus	Possibly from S-E Asian pigs
1997	H5N1 influenza virus	Avian 'flu from Hong Kong and China
1997	variant Creutzfeldt-Jakob disease	"Mad-cow disease"
1997	Australian bat lyssavirus	Rabies-like
1995	HHV-8 virus	Kaposi sarcoma virus
1993	Hantavirus	S-E USA deer mouse
1991	Sabia virus	Brazilian hemorrhagic fever? rodents
1991	Guanarito virus	Venezuelan hemorrhagic fever
1988	Hepatitis C, hepatitis E, and HHV6	
1982	HIV	AIDS: 47 million now infected
1982	E. coli O157:H7	Enteropathogenic E. coli
1977	Campylobacter jejuni	Severe food poisoning
1977	Ebola virus	Origin in central Africa

PHYSICIAN PREPAREDNESS

There has, until recently, been poor involvement of health care professionals and health care facilities in disaster preparedness [37] as the strategic risks of BT were thought insufficient to justify the considerable investment required to mitigate a major BW attack. In these changing circumstances, accurate and rapid diagnosis of these usually unfamiliar diseases by all physicians has to be a principal goal. Primary responders must have a high level of suspicion as well as a high level of knowledge of putative agents, yet most physicians have had no training to identify BW exposure.

Training needs to be institutionalized in schools of medicine and schools of nursing, by also providing courses at county, state, and national medical society meetings, and as part of specialist board certification/ recertification, and for state licensure. A health education coalition on bioterrorism has been convened by the Association of American Medical Colleges (AAMC) in partnership with CDC and the American Medical Association (AMA) to develop educational materials in BT for health care professionals. The American College of Emergency Physicians (ACEP) are conducting courses for their crucial constituents. An 8-hour Department of Justice (DOJ) technician-hospital provider training course is available through the National Domestic Preparedness Office (NDPO) in designated cities. Many physicians are currently unfamiliar with the appropriate lines of communication in the event of seeing a patient with a suspicious disease pattern. Extensive databases and national expertise can be accessed in an emergency by telephone at 1-800-424-8802.

MICROBIOLOGY LABORATORY PREPAREDNESS

There are 158,000 laboratories in the US that serve the medical community and consequently might be involved in a BW attack. Automated microbial identification systems, that are used routinely, perform poorly on BW agents and specific testing is therefore necessary. Biosafety facilities are minimally required to culture these organisms and many smaller facilities are lacking them. Most hospital and clinical laboratories are Level A facilities which are expected to be able to rule out BT pathogens [38]. Screening algorithms have recently been devised by the American Society for Microbiology (ASM) and the CDC to rule out five high-priority BT agents, and tests to exclude other BW pathogens are being developed. Clinical diagnostic cultures can be done at this level for anthrax, plague, tularemia, and brucellosis. Larger microbiology laboratories are being encouraged to increase their instrumentation and skill levels to allow much greater testing within community laboratories, a critical element to save time (and money) during any outbreak of infectious disease.

Level B laboratories are found in the biggest urban health facilities and in some County and in all State Public Health Laboratories. These facilities can confirm the identification of suspicious isolates and determine their *in vitro* antimicrobial sensitivity. PCR (polymerase chain reaction) methodology, developed for the rapid diagnosis of these agents by CDC, will increasingly be available.

Level C laboratories are facilities that include immunodiagnostic testing, phage typing, and toxigenicity testing. Level D microbiology laboratories are found at CDC, at the US Army Medical Research Institute in Infectious Diseases (USAMRIID), Fort Detrick, MD, and in a few other federal agencies. These laboratories incorporate advanced molecular techniques and have considerable built-in redundancy in case of need [38]. Live smallpox and the viral hemorrhagic fevers are exclusively investigated in level D facilities, although specimens can be sterilized and utilized in specific PCR techniques in lower level laboratories.

The qualifications, supervision, and experience of microbiology staff are variable across the US and hence the capability to detect unusual infectious agents. To some extent, this has been an inadvertent result of the economies necessitated by managed care. If there is one factor likely to enhance early detection of BW pathogens, it is the development of close professional relationships between clinicians and microbiologists in the routine diagnosis of serious infection. The importance of professional training for microbiological staffs in BW is reflected in the training programs and materials that have been devised by federal agencies such as the CDC, and by professional organizations, including AAMC, the Infectious Disease Society of North America (IDSA), National Laboratory Training Network (NLTN), Association of Public Health Laboratories (APHL), and the National Association of Clinical Laboratory Scientists (NACLS). Outcome measures need to be incorporated, such as in the laboratory proficiency testing administered by the College of American Pathologists (CAP). Biosafety remains a serious issue in many laboratories.

Clinical microbiology laboratories must develop a BT Preparedness Plan to anticipate all eventualities and which becomes part of the standard hospital disaster plan. The Laboratory Director puts the contingency plan into operation as soon as a BT event is suspected. It should include:

- Risk analysis checklist for the laboratory
- Vaccination policies and list of OSHA (Occupational Safety and Health Administration) safety measures, including personal protective clothing
- Post-exposure vaccination, drug prophylaxis, and prospective care policies
- FBI chain-of-command and evidence documentation for isolates
- Measures to ensure security of and to limit access to isolates
- Standard BT candidate agent protocols [39]
- Use of universal precautions and containment facilities, e.g., biosafety cabinets
- Autoclaving or incineration of infected material; instrument disinfection protocols
- Ongoing preparedness training program descriptions
- Levels of stock supplies and sourcing of emergency supplies
- Storage and emergency sourcing of packaging materials; training in specimen transportation in accordance with IATA (UN 6.2) packaging regulations; utilization of secure courier systems
- Location of state and federal reference laboratories with round-the-clock contact numbers
- Location of nearest laboratory capable of confirmatory identifications
- Official log of hospital, local government, law enforcement, and EMS contact numbers
- Policy establishing official administrative spokesman for all inquiries

The methodologies of dealing safely with BT pathogens are very labor-intensive and reserve capacity must be created. Federal support is currently inadequate. Busy laboratories on tight budgets must maintain routine operations and yet develop complex capabilities necessary to support the rapid, accurate, and safe diagnosis of rare dangerous pathogens [40]. The dissemination of PCR techniques to afford rapid diagnosis is a high priority.

The National Laboratory Response Network (NLRN) for bioterrorism is being established with federal funding as a secure computer network between members of APHL, CDC, the CDC Rapid Response and Advanced Technology Laboratory (RRAT), the CDC Environmental Health Laboratory for Chemical Terrorism (EHLCT), FBI, DOD, the state and local public health laboratories, and the nation's clinical laboratories [41]. The network is designed to integrate expertise in rare and lethal biological agents into the response to every biological emergency.

INFECTION CONTROL/ HOSPITAL EPIDEMIOLOGIST PREPAREDNESS

The infection control community is responsible for assuring the safety from infection of patients, staff, and public within hospitals. They also work closely with the department of infectious disease in coordinating the hospital emergency response to epidemics. Infection Control Officers are involved in many aspects of hospital operations, not least in studying patterns of infective disease, in conjunction with the Hospital Epidemiologist, from which the first suspicions of an unnatural BW attack rather than a natural event may emerge.

Moreover, the safety of the hospital and its staff are paramount if the hospital is to continue functioning. Vaccination, prophylactic drug treatment, and postexposure protocols must be in place, together with a hospitalwide plan for implementation. Families of hospital workers probably also ought to be treated. Other responsibilities include the development and enforcement of the use of universal precautions, protocols on isolation of patients, on the use of disease-specific protective equipment and eye protection, policies for patient placement that control for the availability of security, housing, closed ventilation systems, plumbing, and waste disposal, and predetermined plans for triage, patient transportation, cleaning, disinfection, sterilization, discharge management, and post-mortem care [42]. The Infection Control Officer, Infection Control Committee Chairman, or designate is empowered to rapidly implement preventive and containment measures in response to an infectious disease outbreak. There is the same unmet need for education and training in BT threats among infection control and hospital epidemiologist professionals as among other front-line physicians.

MEDICAL EXAMINER AND CORONER PREPAREDNESS

Medical examiners and coroners occupy an important position in national surveillance for unusual causes of infectious disease mortality given their state-derived statutory authority to investigate suspicious, sudden, or unexplained deaths. Autopsies are an effective method of obtaining an accurate diagnosis of deaths caused by infectious diseases or toxic exposures, and should be undertaken in all cases of death of uncertain causes presumed to have an infective etiology. Postmortem examination may reveal characteristic findings, such as hemorrhagic mediastinitis in pulmonary anthrax, and also assures thorough laboratory investigation. Both professional groups are skilled in preserving medicolegal evidence. In common with all other medical first responders, education and training programs directed to the specific and separate requirements of medical examiners and coroners are needed [43]. In addition, improved autopsy facilities are necessary in many facilities to ensure that prosecutors are protected from infectious diseases. Mass BW casualty planning must be undertaken in each jurisdiction, and also involve the local mortuary services.

REPORTING A SUSPECTED BIOTERRORISM EVENT

It is likely that the first suspicion of a possible BT attack will occur among hospital professional staff. It may well be inappropriate to await diagnostic confirmation because the consequences of delay may be very serious, should an epidemic be later established. This is a 24-hour day, 7-days-a-week responsibility. The case for notification should be decided by the Infection Control Officer in consultation with infectious disease specialists, clinicians, and laboratory director. Notification of suspicious findings must include hospital administration, CDC, FBI, and local and state public health authorities. Criteria include:

1. one or more cases diagnosed with:
 - Suspected smallpox or anthrax
 - Uncommon agent or disease occurring without explanation, e.g., *Burkholderia mallei* (glanders) or *pseudomallei* (melioidosis), pulmonary anthrax
 - Microbial isolate with markedly atypical features
 - Illness due to aerosol, food, or water sabotage
2. one or more clusters of unexplained illness

The State Governor is responsible for declaring a state of emergency. The CDC and FBI will coordinate the decision of whether to declare a suspected bioterrorist attack.

HOSPITAL PREPAREDNESS

US Hospitals have all-hazards disaster management plans in place in accordance with the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and at least one major drill must be conducted per annum. These plans are tailored to the needs and assets of each community and are coordinated with the emergency medical services, law enforcement, fire department, and local government. Disaster management planning is a continuing process and considerable effort is being made to incorporate planning for catastrophic incidents, including a major BT attack.

In contemplating BW mass casualties, hospitals need to plan for circumstances in which their facilities may well be overrun by a sustained demand for sophisticated health care and by a host of worried as well. Planners need to consider that patients may have to be cared for in unconventional but secure alternate sites close to the main facility. Hospitals may need to quarantine, divert incoming patients, or evacuate. Maximum utilization has to be maintained, to be supplemented by regional, state, and federal assets. Around-the-clock multiple shift capabilities with additional expansion of selected hospital operations must be provided for. It must

be taken into consideration that personnel may be unavailable, perhaps part of the epidemic, and skilled temporary replacements sourced. Shortage areas such as RNs, laboratorians, and pharmacy are especially problematic. New staff shortages and organizational difficulties can be expected during the disease outbreak.

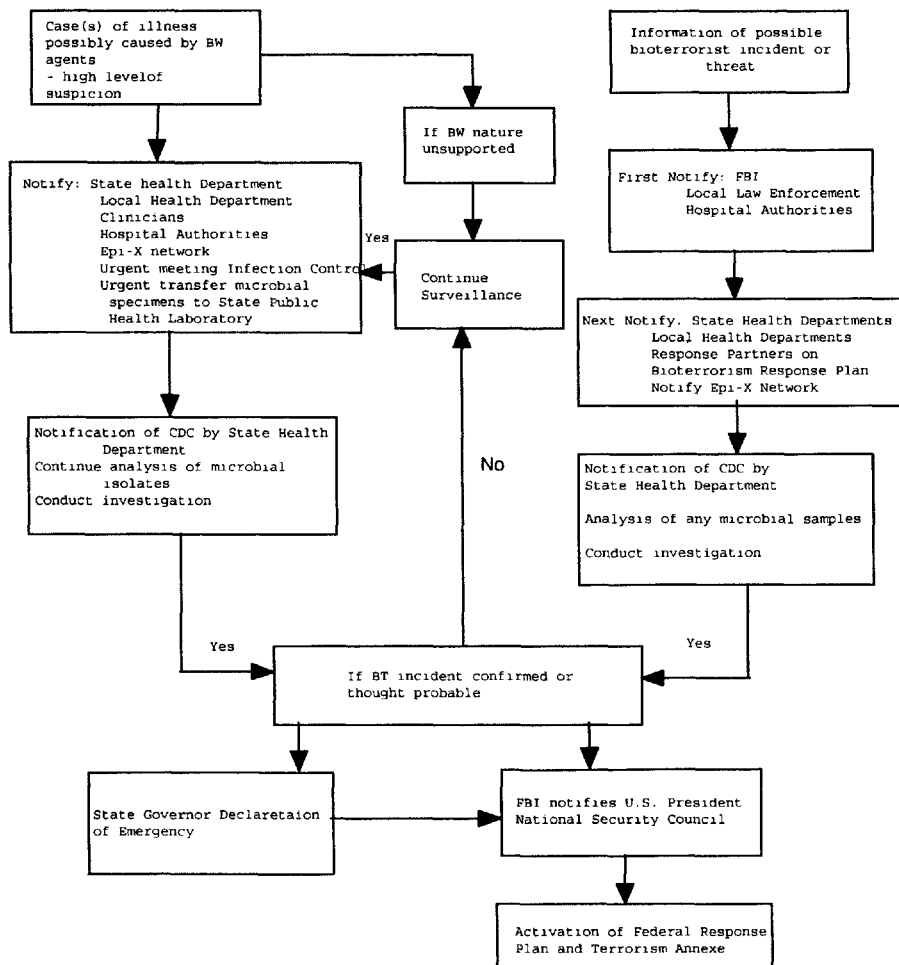


Figure 26.1 Protocol for notification.

Outside aid will probably be essential. Important components of hospital BW planning [29,44,45] include:

- Hospital disaster plans to include BW responses,

- Telephone connections and internet access may be swamped. Therefore secure radio and electronic communications to public health services, EMS, local and state government, law enforcement, regional health assets, CDC, FEMA, and the local media are needed,
- Emergency department personnel, infectious disease and infection control specialists, microbiologists, and the medical and nursing staffs must be educated to be alert to unusual infectious disease manifestations,
- Planning for efficient internal communications, with a dedicated staff, phones, FAX, and dedicated secure internet connections; built-in communication redundancy,
- Medical surveillance and epidemiology infrastructure in place,
- BW infection control and microbiology protocols incorporated,
- Pharmaceutical and antibiotic reserves to be actively monitored; plans to increase surge capacity,
- Maintenance of rosters of essential emergency personnel; organization of volunteer personnel; up-to-date listings of volunteer physicians, retired medical and nursing professionals and medical students; consideration of annual familiarization course,
- Dedicated decontamination facilities with planning for rapid enhancement when necessary,
- Plans for hospital lockdown; disposal of contaminated material; additional mortuary facilities; auxiliary power; increased fuel storage capacity; enhanced security,
- Personnel protection supplies will need to be rapidly augmented,
- Medical and pharmaceutical supplies including antibiotics, antitoxins, ventilators and other supplies to be stockpiled; emergency sourcing in place,
- Mental health resources to treat family members of casualties and to care for the corps of responders,
- Regional plan for all health facilities to work as a team and to increase surge capacity. This may include planning for the exclusive use of certain facilities as fever hospitals; for patient triage; the transfer of patients between institutions; and the use of emergency makeshift facilities such as hotels, civic halls or sporting arenas as hospitals, with other facilities used to conduct screening and prophylaxis. Veterans Administration facilities will be an integral part of regional planning under the VA 4th Mission. These emergency planning concepts are part of the DOD-proposed Modular Emergency Medical System (MEMS) [8] (See Figure 26.2),
- Training and drills necessary to maintain preparedness, and
- Hospital Incident Management Command Center familiar with local, state, and federal disaster planning.

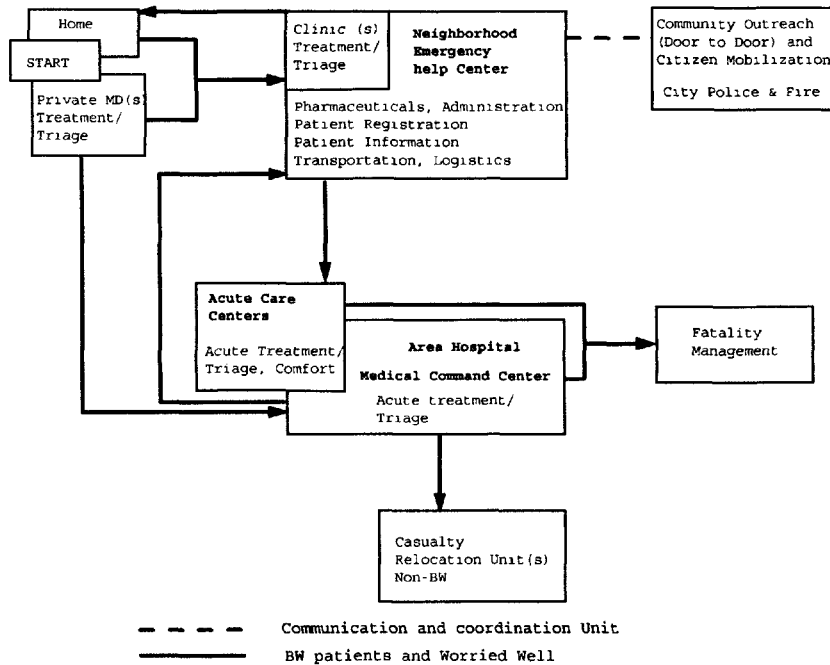


Figure 26.2 Emergency planning concept.

The DHHS Office of Emergency Preparedness (OEP) is developing a federal Metropolitan Medical Response System (MMRS) to help provide a unified response to mass casualty events. Concentrating on major cities, 122 have so far received training and testing programs to build upon existing local emergency response programs and incorporate all local assets. However, the avoidance of state and county institutions has drawn criticism on the basis that wider dissemination of skills throughout their jurisdictions would have been fostered.

One of the difficulties of establishing true hospital BW preparedness is the current inadequacy of federal funding that has yet to support systematic efforts in the hospital sector. Federal support will be necessary in a system already constrained by managed care, unremunerated indigent care, and by numerous unfunded federal and state mandates. The indemnification of private entities in a disaster is tied to the presidential authority to declare a national emergency.

LOCAL CIVIC PREPAREDNESS

Local preparedness has to be depended upon over the first few days of any disaster response as the full weight of state and federal resources are mobilized. Before an emergency is declared by a state governor, the mayor has full controlling authority, and provides an essential component of the response thereafter. Good planning can prevent jurisdictional conflicts.

Each local authority is encouraged to develop a comprehensive all-purpose disaster management plan. There are approximately 3,000 local public health departments in the US and 75% serve populations of 50,000 or smaller [46]. The median size local health department employs 13 staff and the mean size is 67 employees. Most are agencies of local government and state health authorities have little leverage to improve them; communications between the two entities may be minimal. In 16 states, mostly in the East and Southeast, local health departments are mostly or entirely run as offices of the State Department of Health [46].

In the majority of local health departments, staffing levels are pared back with little or no spare capacity and resources are inadequate. It is obvious that federal and state investment will be necessary at this level [47]. Training courses at the regional and local level must be arranged and professional personnel and equipment increased. Another substantial need is to establish 2-way communication connections into the BT internet-based networks with enhancement of information flows. Local health departments are to be integrated within regional disaster planning. Involvement in the dissemination of information to the general public, in disease surveillance, and in mass vaccinations are essential parts of the local BT response. Familiarity with the local community is an invaluable asset.

Municipal leadership must become cognizant with the potential consequences of BW attack even though more pressing local realities will generally take precedence. The potential consequences of BW demand a respectful hearing, even in rural areas. Consequent demands upon local authorities include coordination of fire, EMS, law enforcement, transportation, personnel management services, and the Red Cross. Special training is needed to develop a health emergency capability in addition to the usual disaster relief orientation [11, 48]. These agencies will be highly motivated to protect the community they serve. Local mutual assistance agreements between adjacent municipalities and counties enhance overall responsiveness. The State Emergency Management Agency (SEMA) usually maintains the local emergency plans on file.

STATE AND STATE PUBLIC HEALTH SERVICE PREPAREDNESS

All the states have organized their disaster response capabilities under the SEMA which has the responsibility for emergency preparedness within state borders and for developing the State Emergency Plan. Until recently, few SEMA had included state health departments in the planning process. In some states, the

SEMA is under the authority of the state's National Guard, which mans the facility. The plan coordinates all state and local responders in a unified disaster response.

The State Governor has full authority within the State. In emergencies, federal assets are not deployed until requested by the Governor. However, when a national emergency is declared by the President under the Stafford Act, the Governor cedes leadership under the Incident Command System (ICS) to the Federal On-Scene Coordinator (FOSC), which in the case of a BW attack will generally be the FEMA OSC. State and local authorities are well represented in the unified command structure. A case can be made for developing a modified command structure to accommodate the realities of a biological event where there may be no disaster 'site.'

An increasingly important role for the SEMA is to ensure that validated training and educational materials in BW preparedness are disseminated throughout the state. This role is to be enhanced with new federal funding. The extraordinary multiplicity of training programs that were developed following the 1996 Nunn-Lugar-Domenici Act were not very effective at reaching the front-line personnel [49], but have been consolidated and redirected with some major programs now under state direction. Training at the state level is much more able to respond to local realities.

The US public health services have suffered from at least 30 years of deferred maintenance [50]. This state of "disarray" is summarized in a 1988 Institute of Medicine report entitled "The Future of Public Health" [51]. Although only moderate amounts of federal funding have so far reached below the level of the state agencies, with the notable exception of the MMRS, there have been considerable improvements in developing public health capability at the state and federal level as a result of the 1997 Domestic Preparedness Program (DPP).

The strongest argument for building up the public health infrastructure as a primary component of the national defense strategy against BW attack (hopefully a rare event) is that a comprehensive infrastructure will also be an invaluable asset to combat the spectrum of national health problems. The 1918 influenza epidemic killed 40M people worldwide and there can be no doubt that pandemics will occur in the future. The HIV epidemic also serves as an example where public health preparedness would have led to earlier containment measures. A system that endows a network of reference microbiology laboratories and epidemiologists establishes effective, proactive disease surveillance at the local level, coordinates training and communication across the state and to relevant jurisdictions, including veterinary services, establishes a framework around which the consequences of a bioterrorist attack or a natural epidemic can be managed effectively, and one to which federal and state emergency assets can more easily be integrated. Communications enhancements are required at all levels of the system, to interconnect with the response partners, and with which to help coordinate education of the general public [52].

The state public health laboratories are a critical resource that is being re-vamped with federal dollars as part of BT preparedness. This will ensure the capability of being able to identify rapidly almost all BW agents. The CDC Infectious Disease Fellowship Program has been a useful source of trained manpower. The needs of physical upgrading of facilities, increased personnel, the provision of diagnostic molecular biology equipment, and providing for reserve capacity are being met.

The infectious disease surveillance capabilities of most public health services have been permitted to decay. A 1999 General Accounting Office (GAO) Report [53] records that most state public health departments had no professional epidemiologist to conduct active surveillance of infectious disease occurrences and half had insufficient staff to conduct regular surveillance of currently known emerging infectious diseases, such as hepatitis C virus and drug-resistant *Streptococcus pneumoniae* [54]. Once a dangerous pathogen is identified, epidemiological investigations seek to determine when and where exposure took place and whether infection is still occurring. By determining numbers of proven cases, attack rates, and the epidemic curve, the magnitude of the problem is uncovered, and the response to containment measures followed. It is particularly important that the implications and limits of data are understood by the non-specialist disaster managers. Vaccination campaigns, mass antibiotic distribution, isolation, quarantine, control of transportation, closure of public places, and the emergency provision of services may be heavily influenced by timely, robust epidemiological data.

There has been no standard method of epidemiological reporting, much of which has been by mail. The 1999 GAO Report [53] quoted, as an example, the fact that CDC used over 100 data systems in monitoring health events, often with differing hardware and software requirements. Many of the programs required state reporting, with the same inefficiencies and potential loss of data. An integrated state-based National Electronic Disease Surveillance System (NEDSS) is being developed to enhance the accuracy and timeliness of disease surveillance reporting.

Two other federal programs administered through CDC are helping to provide an efficient public health communication system; both need to be expanded systematically to the local level. The Health Alert Network (HAN) is a high-speed electronic internet platform to support communications between local, state, and federal assets, to provide a portal for standardized public health training, and to provide distance-based learning technologies. The Epidemic Information Exchange System (Epi-X) is a secure system with round-the-clock coverage to report and discuss preliminary information concerning disease outbreaks and other events related to bioterrorism across jurisdictions [55]. Epi-X provides a rapid means of contact with key officials, real-time access to expert opinion, a secure conduit for patient-related data, and constitutes an important component of a proactive surveillance system designed to provide early identification of BW events. NEDSS and Epi-X run on the HAN system. The established PulseNet network is

available to compare the investigational "fingerprinting" of organisms across the US and Europe.

Syndromic and symptom surveillance prototypes are also being evaluated. Prospective real-time data are collated electronically from such sources as emergency rooms, reports from physicians, sentinel hospitals, and coroners, hospital admissions, ambulance runs, numbers of index laboratory tests, and pharmacy sales of certain medications. The possibility of assuring a more sensitive infectious disease surveillance system is being assessed against the substantial costs and deviation of public health effort [11, 56].

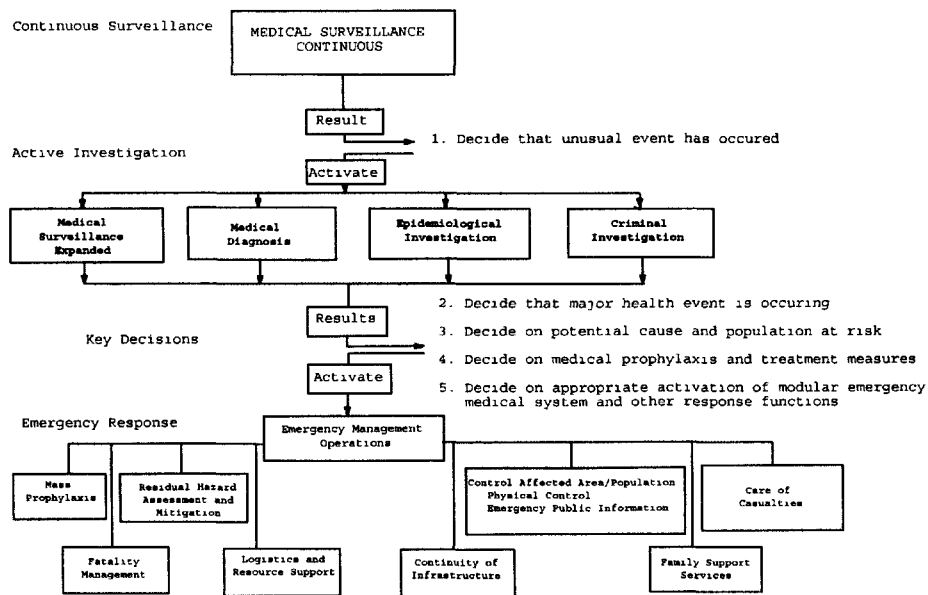


Figure 26.3 Continuous medical surveillance protocol.

The general public must be treated as a key partner in the medical and public health response to bioterrorism [57]. This is likely to be most effective if the information sharing is undertaken close to home, supplemented with national sponsorship. A population informed as to its hidden dangers and informed how it can best care for itself in emergencies is more likely to support advice during an epidemic. The smallest political unit with which all are familiar is the voting precinct. Organization at the precinct level of volunteers, based perhaps around public health nurses and ministers of religion as part of the Citizen Corps, could provide a useful community resource, with periodic training sessions. In a major BT attack, prophylactic drug distribution, community screening, vaccination, and even food distribution might be affected using such a precinct network. Given the inho-

mogeneity of local health services, such statewide local volunteer organization might be better coordinated at state level. The importance of rapid, authoritative, and consistent public communications with the public in any ongoing disaster cannot be overestimated.

In addition to federal agencies, state and local BT response planning needs to involve the following entities:

- public health agencies
- city/ county/ state government
- school systems
- emergency management agency
- environmental agencies: fire; health; water; air quality; consumer safety
- health organizations: hospitals; urgent care centers; physicians; nursing homes; custodial care facilities; home health care providers; pharmacies, poison control centers; mental and occupational health centers
- local emergency planning committee
- National Guard
- private sector: trade and business organizations; industry; labor
- public information office
- public safety: fire; police
- public works/ sanitation
- transportation systems
- volunteer organizations, e.g., Red Cross
- veterinarians

The CDC posted a health alert to public health agencies in November 2001 suggesting jurisdictional contingency planning in the following areas, and requesting that that operational performance be assessed by multiple on-going exercises by which to amend the plans:

- Ensure emergency response plan is authorized by governmental jurisdiction
- Identify facilities suitable for emergency operations centers
- Identify alternative treatment facilities
- Plan for evacuation and relocation of individuals and agency
- Roster of laboratories capable of handling specimens
- Roster of medical facilities capable of handling casualties
- Roster of veterinary laboratories capable of handling specimens
- Roster of veterinary facilities capable of handling infected animals
- Guidelines for addressing environmental decontamination issues
- Safety guidelines for workers dealing with infected people or animals
- Mutual aid agreements with surrounding jurisdictions, including VA and military installations

- Procedures for assisting special populations needing medical care during emergency
- Capabilities for incident stress counseling for victims and response personnel
- Protocol for decontamination of patients on arrival at treatment facility
- Protocol for decontaminating mass casualties (mainly chemical/toxin attacks)
- Protocol for instituting mass isolation within a health facility
- Procedures for organizing and coordinating volunteers during a disaster
- Tested plans for instituting mass vaccination or medication distribution from National Pharmaceutical Stockpile (NPS), including prioritizing first responders and medical/ health care providers
- Protocol for responding to mass mortuary needs

FEDERAL HEALTH AND MEDICAL SERVICES PREPAREDNESS/ OPERATIONS

Where possible, domestic preparedness should rely on existing systems of all-hazards management in which an effective federal response capability has developed over the last 15 years and been honed by considerable experience. The deployment of massive federal support for local and state emergency management assets and the requirements of FBI investigation are common to all terrorism responses. What is different in the planning of a BT response may be the initial absence of a crime scene, casualties that are difficult initially to discern-but which may expand exponentially into an epidemic, the complexity of medical consequence management, and the profound degree of economic and social dislocation possible.

The command structure ought to reflect the fact that this is primarily a medical and public health crisis within a disaster. The Incident Command System (ICS) [58] for a BT event should ideally reflect this reality. Lessons were learned in the recent limited anthrax attack via the mail system, in which CDC was isolated from the ICS and involved public health authorities had occasion to purposely bypass the command structure to obtain information from federal agencies [59]. Another insight is gained from the 2000 TOPOFF exercise centered around a fictional BW plague attack on Denver [60]. The lack of familiarity with the incident command system of the medical leadership and the reluctance of public health officials to give advice in the middle of a burgeoning epidemic in the absence of solid scientific data were identified as major command and control problems. This study also recognized the likely imperative that political leadership will be necessary to provide moral and legal authority when highly consequential decisions have to be taken.

Federal resources are deployed only after the declaration of an emergency by the state Governor, advised by the state Office of Emergency Management.

Exceptionally, assets might be predeployed if intelligence suggested the likelihood of an attack. A presidential declaration is required under the Stafford Act for the FRP to be activated. With real-time improvements in medical and public health surveillance achievable, differing interpretations at state and federal level could possibly bring jurisdictional conflicts into relief. Once a presidential declaration is received, a Federal Coordinating Officer (FCO) is appointed to lead the response. Emergency Preparedness Liaison Officers (EPLO) assist the state and federal agencies in the assignment of specialized and strategic federal assets. The FBI and FEMA are likely to be mobilized simultaneously in BT to coordinate the crisis and consequence management functions.

The operations of the National Response Plan [7,61] are considered in Chapters 10, 23, and 25. This section will concentrate on the role of the Health and Medical Services Response in a BT attack. Considerable consequences may have been predetermined before the nature of the attack is discerned. At this stage, the de facto leadership is held by the health service and local government. The leadership of further consequence management will transfer to FEMA as soon as an emergency is declared. Major consequences of the outbreak will be limited by the successful medical treatment of victims and by the containment of the epidemic, primarily a medical and public health matter. The logistics of this response are rightly the responsibility of the FRP. In a prolonged civilian emergency, it is important to retain the authority of mayors and state governor.

The actions of FEMA are guided by the FRP and the 1997/2000 Terrorism Annex. The Emergency Support Function (ESF) #8 empowers the Department of Health and Human Services (DHSS) to fulfill the public health and medical requirements identified by state and local governments through its executive agent, the Assistant Secretary for Health (ASH) and the Principal Deputy Assistant Secretary for Health (PDASH). The HHS Office of Emergency Preparedness (OEP) is the action agent that will coordinate and facilitate the ESF#8 response. The regional DHHS health administrators (RHAs) are the operating agents. Each support agency will contribute to the overall response, but will retain control over their own resources and personnel.

The HHS Emergency Operations Center (EOC) will be activated within 12 hours of notification. A core staff of pre-designated EOC staff and representatives from the Assistant Secretary of Defense (Health Affairs), DOD, the Undersecretary for Health, VA, and the Director of FEMA will be supplemented by federal partners and other high-level agencies and non-governmental organizations, as appropriate. Special expert advisory groups will be assembled for consultation with the EOC as needed. Support agencies are put onto alert and communication networks are activated. A self-supporting ESF#8 Management Support Unit (MSU) will be deployed to the regional ESF#8 to provide long-distance emergency communications.

FEMA will also have mobilized its central and regional resources, on which the DHSS will have senior representation. The command structure is based upon incident command system principles. FEMA determines which agencies will need

to be represented on its Joint Operations Center (JOC) Command Group, its JOC Consequence Management Group, and on the Joint Information Center (JIC) staff. FEMA may activate an Emergency Support Team (EST) that provides a headquarters interagency coordinating team for the deployment of federal assets. The Catastrophic Disaster Response Group (CDRG) is an interagency advisory re

Table 26.1 Federal Partners Under ESF #8.

DHHS Office of Emergency Preparedness	Federal Emergency Management Agency
Department of Justice	Food and Drug Administration
National Domestic Preparedness Office	National Security Council
Federal Bureau of Investigation	Department of State
Office of Justice programs	Department of Energy
Department of Agriculture	Department of Defense
Department of Transportation	General Services Administration
Department of Veterans Affairs	US Postal Service
National Communication System	Agency of International Development

source. The complex nature of the FRP command structure is illustrated in Figure 10.1 and abbreviated in Figures 24.2 and 24.7.

The initial federal asset dispatched to the incident site(s) is the FEMA Emergency Response Team-Advance Element (ERT-A) that both supports the state EOC and identifies suitable infrastructure in which to set up operations. A Regional Operating Center (ROC) is formed by the FEMA Regional Director to coordinate the early response, to be replaced if warranted by an interagency Emergency Response Team (ERT). The FCO, State Coordinating Officer (SCO), ERT, federal agency regional representatives, and state and local liaison officers are organized as the Disaster Field Office (DFO).

The RHA establishes a regional ESF#8 office as a coordinating center (CC). The RHA is also represented in the DFO on a 24-hour basis. The CC interfaces with ESF#8 and with state and local public health and with medical authorities. Regular assessments of need, prioritization, and strategic analyses are required in the following areas in order to assist state and local governments-the responsible HHS agency is noted:

- Health and medical needs: Office of Public Health and Science (OPHS)/ Office of Emergency Preparedness (OEP)/ National Disaster Medical System (NDMS) - deploy assessment teams
- Health Surveillance: CDC - monitoring field investigations; advice
- Medical Care Personnel: OPHS/ OEP/ NDMS - Disaster Medical Assistance Teams (DMATs) and National Guard/ Military/ VA teams
- Drugs, supplies, and medical equipment: OPHS/ OEP/ NDMS - National Pharmaceutical Stockpile (NPS); commercial sourcing

- Drug safety: Federal Drug Administration (FDA) - surveillance for unsafe products and equipment
- Biological hazard consultation: CDC - field investigations; treatment consultations; decontamination
- Patient evacuation: OPHS/ OEP/ NDMS - DOD resources
- In-hospital care: OPHS/ OEP/ NDMS - intensive care; regional and national networks
- Worker health/ safety: CDC - decontamination; prophylaxis; treatment
- Public health information: CDC
- Mental Health Care: Substance Abuse and Mental Health Services Administration (SAMHSA)
- Victim identification/ mortuary services: OPHS/ OEP/ NDMS
- Veterinary services: OPHS/ OEP/NDMS - assist veterinary authorities

The regional ESF#8 Coordinating Center will develop and update medical assessments and provide situation reports called SITREPS to the CDRG, EST, JOC, JIC, other ESF EOC, the support federal agencies, the state, and other organizations with a need to know. The CC will mobilize local reserves established in disaster planning and other resources. The Joint Regional Medical Planning Office (JRMPO) or other entity designated by the DOD Defense Coordinating Officer (DCO) will assist requests for the use of a variety of military assets that are pertinent to early management of a BT response.

The national HHS EOC will (i) activate DOD support network, (ii) alert National Disaster Medical System (NDMS) resources to standby basis, (iii) mobilize regional NDMS Federal Coordinating Centers (FCC) to obtain bed availability reports from participating non-federal hospitals, (iv) alert the Global Patient Movement Requirement Center (GPMRC) to collate bed availability, (v) alert the HHS Supply Service Center (SSC), the Defense Logistics Agency (DLA), and other pre-identified sources of medical supplies, (vi) alert national communications and transport agencies, and (vii) obtain weather forecasts and geographic information from ESF#5.

The national HHS EOC can mobilize the regional MMRS, deploy mobile NDMS units called Disaster Medical Assistance Teams (DMATs) for triage, patient care, and patient transportation. Data from local ESF#8, FEMA DFO, various federal officials at the scene, state governor, state health officials, state EMS, state disaster authorities, and regional assets are continuously acquired and analysed. Veterans Administration assets, including hospitals, Emergency Medical Response Teams (EMRTs) and Medical Emergency Radiological Response Teams (MERTS) can be accessed through the VA Emergency Management Strategic Healthcare Group (EMSHG). National Guard units can be activated under Title 36 by the State Governor, and under Title 10 by the US President.

Substantial military assets can be obtained under Title 10 status when requested by a state governor or by a lead federal agency. Skilled reaction teams and medical, transportation, supply, security, engineers, or public affairs units can be

provided. However, use of the military should be considered as a last resort because of potential conflicting responsibilities. The Joint Task Force-Civil Support (JTF-CS) is the focus of BW consequence management requests to the military. Air transportation requests are routed via state authorities to regional ESF#8 and on to the NDMS OSC (on-scene commander). When appropriate, patients will be transferred out to relieve local facilities. Patient transfers are coordinated via the GPMRC utilizing a system of collection points. Patient Transport is undertaken by the 375th Aeromedical Evacuation Squadron based at Scott AFB, IL. Logistical air support is provided by the Department of Agriculture and by other agencies. Considerable human resources and materiel can thereby be transported into the area, as long as the airspace remains open.

An immediate problem in any epidemic is the availability of therapeutic and prophylactic drugs, including vaccines, of protective clothing, and of respiratory ventilators. CDC has established the National Pharmaceutical Stockpile (NPS) with a goal of transporting a "push pack" to the local site within 12 hours of federal authorization. The pushpack contains antibiotics, essential medical supplies, and ventilators. The VA manages the pharmaceutical inventory of the stockpile. Additional pharmaceuticals are stored at manufacturers' warehouses in the Vendor Managed Inventory (VMI) program. Planning is being incorporated into state and local preparedness plans to manage and distribute the supplies on arrival.

FEMA and each partner agency in the Health and Medical Services Emergency Response have structured operational plans related to biodefense (see Chapters 23 and 25). Much of the logistical management is common to all disasters. After a BW attack, however, there are particular difficulties in real-time assessment, a prolonged intensive response may be required, and there is the challenge to supplement considerably medical and nursing manpower, to provide alternative medical facilities from scratch for surge capacity, and the possible requirement to maintain a small army of support personnel in the midst of an epidemic. Treatment and disease containment may also have to be undertaken across the US and in foreign countries. Indeed, as much effort may have to be expended in infection containment as in patient care. Civilian communications assume considerable importance, as exemplified by New York Mayor Giuliani after the 2001 World Trade Center terrorism. It is crucial to have communications strategies in place to disseminate prompt, consistent, and accurate information.

Finally, the legal ramifications of such issues as the emergency licensing of out-of-state professionals, exemption of certain mandated professional and institutional standards, exemption of certain public security information from open records laws, compulsory vaccination, population-based prophylactic drug distribution, travel restriction, isolation, the institution of quarantine and its conflict with interstate commerce laws, enforced evacuation, emergency appropriation of medical and other facilities, mass fatality management, role of the military and military reserves, and fundamental questions of local, state, and federal authority should be resolved. The legal framework for biological disaster management must be brought up to date.

CONCLUSIONS

Much of the infrastructure and training created to bolster the national capabilities in biological disaster management will directly enhance the public health services. The preparedness of the medical and public health systems for a BT attack will radically improve US capabilities in infectious disease containment. The complexity of the NRP command and control system is not optimal to manage a BT response, and needs to acquire greater understanding of biological events. The strengthening of relationships with law enforcement, fire departments, and other local, state, and federal agencies will engender future social benefits. Development of new vaccines for candidate BW agents and their strategic use will provide the single most cost-effective intervention [62]. Efficient electronic communications will integrate the medical elements of the response and interface with the local, state, and federal levels of emergency management, and with the general public. It is hoped that a flexible national system will evolve capable of responding efficiently to the most dire of BT doomsday predictions. The level of preparedness at all levels will ultimately determine the outcome.

Preparedness for a BW event must be tested at all levels. New technology, new facilities, and comprehensive educational and training programs are especially needed because of historical underfunding. Failure to rise to the challenge of bioterrorism (if still an unlikely risk) could be catastrophic. Apart from the potential for major loss of life and social disruption, the economic case for BT preparedness is convincing. A recent study estimated the possible economic impact of a bioterrorist attack as \$M477 per 100,000 persons exposed to a brucellosis weapon and \$B26.2 per 100,000 persons exposed to an anthrax attack [63].

On January 10, 2002, President Bush signed the \$B2.9 Terrorism Appropriations Bill. On January 31, 2002, HHS Secretary Thompson advised state governors of the proportion of \$B1.1 that will be distributed to the states in the next federal year. The monies will be spent on comprehensive preparedness readiness at state and local levels. Infectious disease surveillance and investigation, hospital mass casualty management, public health laboratories, and communication and reporting capabilities are to be improved. The funding is divided into three programs: (1) CDC-for public health preparedness; (2) HRSA-for regional hospital planning; and (3) HHS OEP-to support the MMRS-80% of the US population will then be covered by MMRS.

Other funding includes further support for the stockpiling of antibiotics (\$M650), to establish and maintain a dedicated BT workforce at CDC, to continue to develop the new CDC Rapid Response and Advanced Technology Laboratory (RRATL), expand the CDC Epidemiologic Intelligence Service (EIS), expand other CDC and National Institutes of Health (NIH) facilities, to expand vaccine programs, and stockpile a national supply of smallpox vaccine by Autumn 2002. There are substantial increases in applied and basic science BW-related research, and in efforts to develop better detection and monitoring technology (DOD) and to improve environmental detection methods for biological agents (EPA).

REFERENCES

1. O.Toole T, Mair M, Inglesby TV. Shining light on "Dark Winter". *Clinical Infectious Diseases* 2002;34:000 Electronically published 19 February 2002. Internet: <http://www.journals.uchicago.edu/CID/journal/issues/v34n7/020165/020165.html>.
2. Henderson DA. Looming threat of bioterrorism. *Science* 1999;283:1279-1282. Internet: http://cas.bellarmine.edu/tietjen/ecology/looming_threat_of_bioterrorism.htm. March 10, 2002
3. Henderson DA, Inglesby TV, Bartlett JG, Smallpox as a biological weapon: medical and public health management. Working Group on Civilian Biodefense. *JAMA* 1999; 281:127-137. <http://jama.ama-assn.org/issues/v281n22/ffull/jst90000.html> Accessed March 10, 2002
4. Cole TB. When a bioweapon strikes, who will be in charge? *JAMA* 2000;284:944-948. Internet <http://jama.ama-assn.org/issues/v284n8/ffull/jmn0823-2.html> Accessed March 10, 2002
5. Department of Health and Human Services. Health and Medical Support Plan for the Federal Response to Acts of Chemical / Biological (C/B) Terrorism: Final Interim Plan. Washington DC: Government Printing Office, 1995. Internet: http://ndms.dhhs.gov/CT_Program/Response_Planning/C-BHMPlan.pdf Accessed March 10, 2002.
6. CDC Strategic Planning Group. Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response. *Morbidity and Mortality Weekly Report* 2000;49(RR-4):1-14. Internet: <http://www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm> Accessed March 10, 2002
7. Federal Emergency Management Agency. Federal Response Plan. Washington DC: Government Printing Office, 1999. Internet: <http://www.fema.gov/r-n-r/frp/frpfull.pdf> Accessed: March 10, 2002
8. Department of Defense. Improving Local and State Agency Response to Terrorist Incidents Involving Biological Weapons. Washington DC; Government Printing Office, 2000. Internet: http://www.chem-bio.com/resource/2000/bwirp_interim_plan_guide.pdf Accessed March 10, 2002
9. Anonymous. United States Government Interagency Domestic Terrorism Concept of Operations Plan. Washington DC: Government Printing Office, 2001. Internet: <http://www.fema.gov/r-n-r/conplan/conplan.pdf> Accessed March 10, 2002
10. Cilluffo F, Cardash S, Lederman G. Combatting Chemical, Biological, Radiological, and Nuclear Terrorism: a Comprehensive strategy. Washington DC: Center for Strategic and International Studies, 2001. Internet: <http://www.csis.org/homeland/report/combatchembiorad.pdf> Accessed March 10, 2002

11. Smithson AE, Levy L-A. Ataxia, the Chemical and Biological Warfare Threat and the US Response. Stimson Center Report No. 35. Washington DC: Henry L Stimson Center, 2002. Internet: <http://www.csis.org/homeland/reports/combatchembiorad.pdf> Accessed March 10, 2002
 12. Henderson DA. Bioterrorism as a public health threat. *Emerging Infectious Diseases* 1998;4:488-492. Internet: <http://www.cdc.gov/ncidod/eid/vol4no3/hendrsn.htm> Accessed March 10, 2002
 13. Falkenrath RA, Newman RD, Thayer BA. *America's Achilles Heel, Nuclear Biological, and Chemical Terrorism and Covert Attack*. Cambridge, MA: MIT Press, 1998
 14. Lederberg J, ed. *Biological Weapons: Limiting the Threat*. Cambridge, MA: MIT Press, 1999
 15. Gurr N, Cole B. *The New Face of Terrorism. Threats from Weapons of Mass Destruction*. London: Tauris, 2000
 16. Miller J, Engelberg S, Broad W. *Germs, Biological Weapons and America's Secret War*. New York: Simon and Schuster, 2001
 17. Regis E. *The Biology of Doom*. New York: Henry Holt, 1999
 18. Davis CJ. Nuclear blindness: an overview of the biological weapons programs of the former Soviet Union and Iraq. *Emerging Infectious Diseases* 1999;5:509-512. Internet: <http://www.cdc.gov/ncidod/EID/vol5no4/davis.htm> Accessed March 10, 2002
 19. Hoffman B. *Inside Terrorism*. London, Indigo, 1998
 20. Turchie T. Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Government Reform Committee, 106th Congress, 2nd session, July 26, 2000. Washington DC: Government Printing Office, 2000. Internet: <http://www.homelandsecurity.org/quotes/quote.cfm?Authorid=35> Accessed March 10, 2002
 21. Fenner F, Henderson DA, Arita I, Jezek Z, Ladnyi ID. *Smallpox and its Eradication*. Geneva, Switzerland: World Health Organization, 1988
 22. Tucker JB, Vogel KM. Preventing the proliferation of chemical and biological weapon materials and know-how. *The Nonproliferation Review* 2000;7:88-96. Internet: <http://cns.miis.edu/pubs/npr/vol07/71/tucker71.pdf> Accessed March 10, 2002
 23. Laquer W. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford University Press, 1999
 24. Christopher GH, Cieslak TJ, Pavlin JA, Eitzin EM. Biological warfare. A historical perspective. *JAMA* 1997;278:412-417. Internet: <http://jama.ama-assn.org/issues/v278n5/ffull/jsc7044.html> Accessed March 10, 2002
-

25. Falkenrath RA. Confronting nuclear, biological, and chemical terrorism. *Survival* 1998;40(3):43-65
26. Weiner SL. Strategies of biowarfare defense. *Military Medicine* 1987; 152: 25-28
27. Noah DL, Sobel AL, Ostroff SM, Kildrew JA. Biological warfare training; infectious disease outbreak differentiation. *Military Medicine* 1998;163:198-201
28. United States Army Medical Research Institute of Infectious Diseases. Medical Management of Biological Casualties Handbook (the Blue Book), 4th Edit. Fort Detrick, MD: USAMRIID, 2001. Internet: <http://www.nbc-med.org/SiteContent/HomePage/WhatsNew/MedManual/Feb01/handbook.htm> Accessed March 10, 2002
29. Brown B, Meltzer AJ. Medical response to biological terrorist attack. In: *Countering Biological Terrorism in the U.S.: an Understanding of Issues and Status*. Siegrist DW, Graham JM, eds. Dobbs Ferry, New York, Oceana Publications, 1999, pp 117-126
30. Osterholm MT. The medical impact of a bioterrorist attack: is it all media hype or clearly a potential nightmare? *Postgraduate Medicine* 1999; 106(2):121-130. Internet: http://www.postgradmed.com/issues/1999/08_99/osterholm.htm Accessed March 10, 2002
31. Camus A. *The Plague*. Gilbert S, trans. New York, Vintage, 1975
32. Saramago J. *Blindness*. Pontiero G, trans. San Diego, Harcourt Brace, 1977
33. McDade JE. Addressing the potential threat of bioterrorism value added to an improved public health infrastructure. *Emerging Infectious Diseases* 1999;5:591-592. Internet: <http://www.cdc.gov/ncidod/EID/vol5no4/mcdade.htm> Accessed March 10, 2002
34. Rabkin NJ. *Combating Terrorism: Linking Threats to Strategies and Resources*. Testimony to the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, July 26, 2000 Washington DC: General Accounting Office, 2000. Internet: <http://www.gao.gov/new.items/ns00218t.pdf> Accessed March 10, 2002
35. Executive Office of the President, Office of Management and Budget. *Annual Report to Congress on Combatting Terrorism*, May 18, 2000. Internet: <http://www.rand.org/nsrd/terrpanel/terror3-screen.pdf> Accessed March 10, 2002
36. Duckworth L. Super agency to tackle threat of holiday diseases. *Independent* (newspaper). London: January 11, 2002
37. Waeckerle JE. Domestic preparedness for events involving weapons of mass destruction. *JAMA* 2000;283:252-254. Internet: <http://jama.ama-assn.org/issues/v283n2/ffull/jed90095.html> Accessed March 10, 2002

38. Snyder JW, Check W. Bioterrorism Threats to our Future. The Role of the Clinical Microbiology Laboratory in Detection, Identification, and Confirmation of Biological Agents. American Academy of Microbiology and American College of Microbiology, 2001. Internet: <http://www.asmsa.org/acasrc/pdfs/bioterrorism.pdf> Accessed March 10, 2002
39. Snyder, ed. Cumitech 33. Biological Agents Associated with Bioterrorism. Washington DC: American Society for Microbiology, 2000
40. Gilchrist MJR. The progress, priorities, and concerns of public health laboratories. In: Biological Threats and Terrorism: Assessing the Science and Response Capabilities. Knobler SL, Mahmoud AAF, Pray LA, eds. Washington DC: National Academy Press, 2002, pp 160-165
41. Lillibridge SR. Restructuring government for homeland security: nuclear/ biological/ chemical threats. Testimony before the House Committee on the Budget, December 5, 2001. Washington DC: Government Printing Office, 2002. Internet: <http://www.hhs.gov/asl/testify/t011205a.html> Accessed March 10, 2002
42. APIC Bioterrorism Task Force and CDC Hospital Infections Program Bioterrorism Working Group. Bioterrorism Readiness Plan: a Template for Healthcare Facilities. Internet: http://bioterrorism.slu.edu/key_references/BioPlan.pdf Accessed March 10, 2002
43. Nolte KB, Yoon SS, Pertowski C (letter). Medical examiners, coroners, and bioterrorism. Emerging Infectious Diseases 2000;6:559-560. Internet: http://www.cdc.gov/ncidod/eid/vol6no5/nolte_letter.htm Accessed March 10, 2002
44. Johns Hopkins Center for Civilian Biodefense Studies. Enhancing bioterrorism preparedness and response post-September 11: interim actions for the medical and public health community. Internet: <http://www.google.com/search?q=cache:zYaDQDAbmalC:www.hopkins-biodefense.org/+&hl=en> Accessed March 10, 2002
45. Petersen R. A review of federal bioterrorism preparedness programs from a public health perspective. Testimony to the House Committee on Energy and Commerce, October 10, 2001. Washington DC: Government Printing Office, 2002. Internet: <http://energycommerce.house.gov/107/hearings/10102001Hearing390/Petersen624.htm> Accessed March 10, 2002
46. Milne TL. Countering bioterrorism threats: local public health perspectives. In: Biological Threats and Terrorism: Assessing the Science and Response Capabilities. Knobler SL, Mahmoud AAF, Pray LA, eds. Washington DC: National Academy Press, 2002, pp 176-178
47. Fraser MR, Fisher VS. Elements of Effective Bioterrorism Preparedness: a Planning Primer for Local Public Health Agencies. Washington DC: National Association of County and City Health Officials, 2001, Internet: http://www.naccho.org/files/documents/Final_Effective_Bioterrism.pdf Accessed March 10, 2002

48. Taylor ER. Are We Prepared for Terrorism Using Weapons of Mass Destruction? : Government's Half Measures. Cato Institute Policy Analysis No. 387. Washington DC: Cato Institute, 2000, pp 1-19. Internet: <http://www.cato.org/pubs/pas/pa-387es.html> Accessed March 10, 2002
49. US General Accounting Office. Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training: Report to Congressional Requesters. March 2000. Washington DC: GAO, 2000. Internet: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB55/gaot-nsiad-00-218.pdf> Accessed March 10, 2002
50. Gibson J. Assessing state and territorial health departments. In: Biological Threats and Terrorism: Assessing the Science and Response Capabilities. Knobler SL, Mahmoud AAF, Pray LA, eds. Washington DC: National Academy Press, 2002, pp 173-176
51. Committee for the Study of the Future of Public Health, Division of Care Services, Institute of Medicine. The Future of Public Health. Washington DC: National Academy Press, 1988
52. Quinlisk P. Combating terrorism: federal response to a biological weapons attack. Testimony to the Subcommittee on National Security, House Committee on Government Reform, July 23, 2001. Washington DC: Government Printing Office, 2001. Internet: http://www.house.gov/reform/ns/107th_testimony/council_of_state_and_territorial.htm Accessed March 10, 2002
53. US General Accounting Office. Emerging Infectious Diseases: Consensus on Needed Laboratory Capacity Could Strengthen Surveillance, February 1999. Washington DC: GAO, 1999. Internet: <http://www.phppo.cdc.gov/mlp/pdf/nls/HEHS-99-26.pdf> Accessed March 10, 2002
54. Osterholm MT. Bioterrorism: our front line response, evaluating US public health and medical readiness. Testimony to the Subcommittee on Public Health, Senate Committee on Health, Education, Labor, and Pensions, March 25, 1999. Washington DC: Government Printing Office, 1999. Internet: <http://www.cste.org/testimony2.htm> Accessed March 10, 2002
55. Bioterrorism Preparedness and Response Program. National Bioterrorism and Response Initiative: Overview and General Information About the Initiative. Atlanta: Centers for Disease Control and Prevention, 2000. Internet: <http://www.bt.cdc.gov/documents/RegMeetingSlides/Overview.pdf> Accessed March 10, 2002
56. Smithson AE. A review of federal bioterrorism preparedness programs from a public health perspective. Testimony to the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, October 10, 2001. Washington DC: Government Printing Office, 2002, Internet: <http://energycommerce.house.gov/107/hearings/10102001Hearing390/Smithson622.htm> Accessed March 10, 2002
57. Glass TA, Schoch-Spana M. Bioterrorism and the people: how to vaccinate a city against panic. *Clinical Infectious Diseases* 2002; 34:217-223. Internet:

<http://www.journals.uchicago.edu/CID/journal/issues/v34n2/011333/011333.html> Accessed March 10, 2002

58. Erickson PA. Emergency Response Planning for Corporate and Municipal Managers. San Diego, Academic Press, 1999, pp 82-102
59. Geberding JL. Lessons learned: the challenges and opportunities. In: Biological Threats and Terrorism: Assessing the Science and Response Capabilities. Knobler SL, Mahmoud AAF, Pray LA, eds. Washington DC: National Academy Press, 2002, pp 149-152
60. Inglesby T, Grossman R, O'Toole T. A plague on your city: observations from TOPOFF. *Biodefense Quarterly* 2, No.2 (September 2000). Internet: www.hopkins-biodefense.org/pages/news/quarter.html
61. Benwell-Lejeune PH. Federal cooperation. In: *Countering Biological Terrorism in the U.S.: an Understanding of Issues and Status*. Siegrist DW, Graham JM, eds. Dobbs Ferry, New York: Oceana Publications, 1999, pp 85-100
62. Russell PK. Vaccines in civilian defense against bioterrorism. *Emerging Infectious Diseases* 1999;5:531-533. Internet: <http://www.cdc.gov/ncidod/EID/vol5no4/russell.htm> Accessed March 10, 2002.
63. Kaufman AF, Meltzer MI, Schmid GP. The economic impact of a bioterrorist attack: are prevention and postattack intervention programs justifiable? *Emerging Infectious Diseases* 1997;3:83-94. Internet: <http://www.cdc.gov/ncidod/eid/vol3no2/kaufman.htm> Accessed March 10, 2002.

Index

- 1,4-Oxazepine (CR), 326
 - 10 U.S.C. 15, 523
 - 10 U.S.C. 331-333, 523
 - 1994 sarin attacks, 434
 - 19th Century terrorists, 27
 - 29 CFR 1910 (Code of Federal Regulations), 448
 - 42 U.S.C. 5121, 507
- A
- AAVLD (American Association of Veterinary Laboratory Diagnosticians), 122
 - Abdominal pain, 82
 - Abrin, 110
 - Abrus seeds, 110
 - Absorption spectroscopy (AS), 389
 - Acceptable losses, 450
 - Acoustic-to-optic tunable filters (ATOTFs), 391
 - Activated charcoal, 457
 - Adamsite (DM), 326
 - Advanced oxidation processes, 417
 - Advanced warning system, 376
 - Advice to civilians, 349
 - Aero 14B, 374
 - Aerodynamic particle sizing (APS), 156
 - Aerosol, 47
 - dispersion, 56, 197
 - impactor, 57
 - interaction with gas molecules, 51
 - tracking, 147
 - Aflatoxins, 110
 - African swine fever, 124
 - Agency for Healthcare Research and Quality (AHRQ), 223
 - Agency for Toxic Substances and Disease Registry. *See* ATSDR
 - Agent Orange, 327
 - Agent properties, 96
 - Agents of biological warfare, 66
 - Agglomerates, 48
 - Agricultural commodities, 121
 - Agricultural Research Service, 122
 - Agriculture, 209
 - Agroeconomic bioterrorism, 121
 - Agroeconomic protection, 127
 - Agroterrorism, 531
 - AIDS, 214
 - Air monitoring, 268
 - Airborne release, 104
 - Airborne transmission, 206
 - Air-purifying respirator (APR), 451
 - Alarm system, 376
 - ALF (Animal Liberation Front), 123, 126
 - Alfred Murrah Federal Building. *See* Oklahoma City bombing
 - Algae, 110
 - Alibek, Ken (Kanatjan Alibekov), 68, 99, 110
 - Alkaloids, 110

- Alpha, 267
 Al Qaeda (al-Qaeda), 64, 104
 American Association of Veterinary
 Laboratory Diagnosticians,
 122
 American Medical Colleges (AMC),
 535
 American Society for Testing of
 Materials (ASTM), 460
 American Type Culture Collection,
 112
 Amherst, 96
 AMRIID. *See* USAMRIID
 Anaerobic, 111
 Anatoxin, 110
 Ancient telegraph, 26
 Andersen impactor, 150
 Andersen microbial sampler, 154
 Animal and Plant Health Inspection
 Service (APHIS), 122
 Animal Health Association, 122
 Animal inoculation, 129
 Animal Liberation Front. *See* ALF
 ANOVA, 133
 Anthrax, 6, 10, 61, 68, 69, 73, 109,
 174, 198, 536
 diagnosis, 70
 hoaxes, 63
 inhalational, incubation period, 70
 outbreak, 11
 spores, 70
 symptoms, 69, 70
 treatment, 70
 vaccine, 72
 weaponization, 99
 Antianimal, 109
 Anti-ballistic missile systems, 288
 Anti-Ballistic Missile Treaty, 288
 Antibody detection, 129
 Antibody-antigen binding, 171
 Antibody-based biosensors (ABB),
 402
 Antibody-coated oscillator (ACO),
 403
 Anti-crop bomb, 97
 Antigen detection, 129
 Antimaterial, 109
 Antipersonnel agents, 109
 Antiplant, 109
 AP2C, 378
 APHIS (Animal and Plant Health
 Inspection Service), 122
 Arab Palestinian groups, 19
 Arenaviridae, 81
 Arenaviruses, 199
 Argentine HF, 81
 Arms control, 288
 Army Chemical Corps, 146
 Army's Technical Escort Unit, 146
 Arrival rate, 310
 ARS, 122
 Artillery, 24
 Artillery shells, 98
 As Low As Reasonably Achievable
 (ALARA), 450
 Asphyxiating, 322
 Assess the Hazards, 448
 Assistant Secretary for Health (ASH),
 549
 Association of Public Health
 Laboratories (APHL), 536
 ATSDR (Agency for Toxic
 Substances and Disease
 Registry), 436
 Atmosphere-supplying respirators,
 453
 Atmospheric conditions, 54
 Atomic Energy Act, 478
 Augmentation Response Teams, 514
 Aum Shinrikyo, 6, 24, 37, 86, 104,
 197, 348, 434, 530, 532
 Australia Group, 117, 437
 Automatic weapons, 23
 Automobile exhaust, 55
 Avalanche photodiodes, 162
 Ayatollah Khomeini, 26

B

- Bacillus anthracis, 109, 155
- Bacillus Globigii, 97
- Bacillus Subtilis var. Niger (BG spores), 159
- Backscatter x-ray, 398
- Bacteria, 109, 125
- Balloons, 56
- Baltimore tunnel, Hazmat fire, 484
- Batch fermentation, 111
- Batch process, 111
- Batrachotoxin, 110
- Battle dress over-garments (BDO), 456
- Becquerel (Bq), 260
- Beirut, 17
- Beryllium, 282
- Beta, 267
- BG. *See* Bacillus Globigii
- Bhagwan Shree Rajneesh, 65
- Bhopal, Madhya Pradesh, India, 435
- BIDS, *See* Biological Integrated Detection System
- Binary shells, 374
- Bin Laden, Osama, 19
- Bioaerosols, 54, 56, 57, 148
 - samplers, 154
- Biocrime, 73
- Biofluorescence, 161
- Bioinformatics, 134
- Biological agents, 61
 - amount need for attack, 103
 - identification, 518
- Biological and Toxin Weapons Convention, 68, 200, 205, 529
- Biological attack, nature of, 532
- Biological incident template, 504
- Biological Integrated Detection System (BIDS), 178
- Biological protection, 459
- Biological warfare, 62
 - future of, 110
 - history of, 161
- Biological weapons (BW), 61, 95
 - calculation of agent mass, 105
 - features of an attack, 533
 - history, 65, 95
 - planning, 540
 - production, 109
 - testing of, 98
 - USSR program, 99
- Biological Weapons Convention, 65, 99, 117
- Biologically active molecules, 378
- Biopreparat, 68, 99
- Biosafety, 536
- Biotechnology revolution, 110
- Bioterrorism (BT), 61, 195, 200
 - preparedness plan, 537
 - response, 547
 - threats, 531
- Bioterrorism Preparedness Response Program (BPRP), 529
- Biotic pathogens, 124
- Biotin, 168
- Bioweaponers, 111
- Black Death, 96
- Blister agents, 322
- Blistering, 356
- Blood agents, 322, 357
- Blowers, 55
- BLU 80/B binary VX, 374
- Boiling point, 340
- Bolivian HF, 81
- Bomb threat checklist, 499
- Bomber, 24
- Bombs, 374
- Boston Tea Party, 17
- Botulinum toxins, 84
- Botulism, 6, 83, 102, 174, 199
 - diagnosis, 85
 - symptoms, 84
 - treatment, 86
- Bragg-Gray chambers, 267
- Brazilian HF, 81
- British Law cyber-terrorists, 297
- Brucella, 99

Brucellosis, 68, 102, 199, 536
 Bt corn, 137
 Bubblers/impingers, 150, 155
 Bubonic plague, 78
 Bunyaviridae, 81
 BW. *See* Biological weapons
 BZ, also known as QNB, 326

C

Caffa, 65, 95
 Camp Detrick, 67, 97
 Canine, 379
 Capability assessment chart, 497
 Castor beans, 110
 Catastrophic Disaster Response Group (CDRG), 476
 Category A BW, 69
 Category B BW, 69
 Category C BW, 69
 CBIRF, 201
 CBRNE, 515
 CDC, *See* Centers for Disease Control and Prevention
 CDRG, 481, 524
 CdTe, 267
 CdZnTe, 267
 Center for Animal Disease and Information and Analysis, 131
 Center for Health Promotion and Preventive Medicine, 514
 Centers for Disease Control and Prevention (CDC), 64, 68, 198, 518, 519
 Central Processing Unit. *See* CPU
 Changteh, 65
 Charged based deep level transient spectroscopy (Q-DLTS), 185, 395
 Charismatic leader, 36
 Chemical and Biological National Security Program, 232
 Chemical agent proliferation, indicators, 439
 Chemical biological mass spectrometer (CBMS), 167
 Chemical-Biological-Radiological (CBR), 23
 Chemical, Biological, Radiological, Nuclear and High Energy Explosives (CBRNE), 466
 Chemical, biological, radiological, environmental defense response teams, 514
 Chemical destruction, 416
 Chemical incident response template, 502
 Chemicals
 properties, 334
 toxicity, 502
 Chemical sensors, 373
 Chemical signatures, 440
 Chemical terrorism, 321
 Chemical weapons (CW), 411, 429
 advantages, 342
 attack, 348
 cloud, 348
 cost of destruction of agents, 412
 delivery, 373
 destruction of, 411
 disadvantages, 342
 disarmament, 432
 hazards, 346
 liquid, 346
 poisoning, 353
 quantity, 412
 quantities of agents, 433
 synthesis, 332
 toxic chemicals and, 322
 toxicities, 346, 355
 Chemical Weapons Convention (CWC), 321
 Chemiluminescence (ChL), 386
 combined with GC (ChL/GC), 387
 Chimera virus, 110
 Chlorine, 323, 346
 Chloroacetophenone (CN), 326

- Chloropicrin, 429
- Choking agents (lung irritants), 322, 358
- Cholera, 102, 109, 174
- Cigarette smoke, 55
- Ciprofloxacin, 70, 79
- Citizen Corps, 546
- Citrus canker, 97
- Cityscapes, 348
- Civilian Research Development Fund, 289
- Class 1 ensembles, 458
- Class 2 ensembles, 458
- Class 3 ensembles, 459
- Clostridium Botulinum, 61, 83
- Coagulation, 56
- Cocco-bacillus, 78
- Collection filters, 152
- Collective memory, 36
- College of American Pathologists (CAP), 536
- Combustion, 55
- Command post, 499
- Commander in Chief, 467
- Commercial chemicals, 322
- Communications, 228
 - technology, 25
- Comotoxins, 110
- Components of computer networks, 304
- Comprehensive Nuclear Test-Ban Treaty (CTBT), 289
- Computers:
 - bacteria, 301
 - chips, 130
 - network, operation of, 306
 - personal, 300
 - programs, 56
 - malicious, 317
 - protection, 316
 - super-computing clusters, 300
 - tomography, 398
 - viruses, 301
 - vulnerability, 299
- Concentration time product (Ct), 346
- Concept of operations, 520
- Condensation, 55
- Conditional exposure, 450
- Conductivity-based sensors (CBS), 396
- Conplan, 204
- Consequence Management (CoM), 466, 475, 492
- Consequence phases, 492
- Contact hazard, 346
- Containment, 259
- Continuing actions, 525
- Continuous fermentation, 111
- Continuous medical surveillance protocol, 546
- Control nuclear transfers, 290
- Convective motion, 54
- Coroners, 538
- Corporate and enterprise intranets, 300
- Counter terrorism, 20, 28
- Countermeasures, 288, 437
- CPU, 306
- Crime scene, 492
- Crimean-Congo HF virus (CCHFV), 81, 110
- Crisis management, 473, 474
- Crisis Management Team, 366
- Criticality, 280
- Crop-dusting, 55, 104, 123
- Cruise missile, 99
 - with spray tank, 374
- Curie (Ci), 259
- Cutaneous, 69
- Cyber-terrorism, 294
 - three levels of capability, 298
- Cyber-economy, 298
- Cyclone sampler, 148, 150, 153
- Cyclones, 55
- Cytotoxins, 110

D

- Dalles, Oregon, 65
- Danger area, 498
- Dark winter, 212
- DARPA, 213
- Data communication, 303
- Data gathering, 378
- Databases, 535
- Data-mining, 134
- DCO, 522
- Decontamination:
 - of casualties, 352
 - of equipment, 417
- Defectors, 68
- Defense against terrorism, 21
- Defense Coordinating Officer, 522
- Defense Reform Initiative Directive #25, 515
- Defoliants, 322
- De-individuation, 40, 41
- Delayed effects, 272
- Delivery system, 99
- Dengue fever, 110
- Department of Agriculture, U.S. (USDA), 122
- Department of Defense (DOD), 513, 529
- Department of Energy (DOE), 516
- Department of Health and Human Services (DHHS), 471, 510, 517, 549
 - Emergency Operations Center (EOC), 367, 549
- Department of Health and Social Services (DHSS), 528
- Department of Justice (DOJ), 473, 510, 528
- Deployed agents, 67
- Deposition, 54
- Deputy Assistant Secretary for Health (DASH), 549
- Dermal protection, 456
- DES (Data Encryption Standard), 319
- Desert Test Center, Salt Lake City, 98
- Desiccants, 322
- Designer virus, 111
- Destructive events, 16
- Destructive power of nuclear, chemical, and biological weapons, 103
- Detection:
 - and analysis, 129
 - of biological agents, 145
 - of chemical agents, 440
 - of clandestine production, 440
 - of metabolic products, 130
 - paper, 377
 - tickets (enzyme), 377
 - time, 378
- Detector systems, 130
- Detergents, 424
- Determine the risk, 448
- Deterrence, 205
 - of terrorism, 21
- DFO, *See* Disaster Field Office
- Diagnosis of serious infection, 536
- Diagnostic kits, 174
- Diamond, 267
- Diarrhea, 82
- Dibenz (b,f), 326
- Differentiation, 378
- Diffusion coefficient, 51
- Di-Methyl MethylPhosphonate (DMMP), 437
- Di-MethylAminoPhenol (DMAP), 358
- Diodes, 267
- Director of Military Support (DOMS), 521, 522
- Directorate for Industrial Production and Scientific Enterprise, 99
- Disaster Field Office (DFO), 494, 522
- Disaster Information Systems Clearinghouse (DISC), 481
- Disaster Medical Assistance Teams (DMAT), 224, 367, 468
- Disasters and emergencies, 465

- Discharging the agents, 100
Disease process, 124
Dispense, 99
Dispersability, 74
Dispersal patterns, 100
Disperse, 99
Dispersion, 56
 dissipation of chemical agents,
 373
Dissemination, 100
Distributed attacks, 124
DNA, 110
 microarrays, 130
 probes, 130
 sequence, 134
 virus, 74
Doctrinal point of view, 450
DOD, *See* Department of Defense
DOJ, *See* Department of Justice
Domestic Emergency Support Team
 (DEST), 474
Domestic loner, 532
Domestic preparedness, 1
Domestic Preparedness Program
 (DPP), 544
DOMS, *See* Director of Military
 Support
Dose, 259
Doxycycline, 79
Drones, 98
Drug resistant, 68
DTC, 98
Dual x-ray source, 398
Dual-use chemicals, 438
Dugway Proving Grounds, 97, 148
Dust, 55
Dynamics, large-group, 38
- E
- Earth Liberation Front. *See* ELF
Eastern equine encephalitis, 110
Ebola, 6, 99, 110, 199
ECD combined with GC (ECD/GC),
 383
Economic espionage, 117
Economic terrorism, 126
Eco-terrorist, 126
ED₅₀, 346
Edema toxin, 69
Education, 3
Eighteen-Nation Disarmament
 Committee, 288
Ekaterinburg, Russia, 71
Electrochemical luminescence, 174
Electrolyte-Insulator-Semiconductor-
 structure (EIS), 176
Electron capture detector (ECD), 381
Electronic resources for bioterrorism,
 88
ElectroSpray ionization (ESI), 164,
 165
Electrostatic devices, 55
ELF, 123, 126
Embedded systems, 299
Emergency planning concept, 542
Emergency Preparedness Liaison
 Officers (EPLO), 549
Emergency responders, 496
Emergency response preparedness
 cycle, 490
Emergency Response Team (ERT),
 470
 Advance element (ERT-A), 479
Emergency rooms, 534
Emergency Support Function (ESF),
 468
 ESF #1, 469
 ESF #2, 469
 ESF #3, 469
 ESF #4, 470
 ESF #5, 470
 ESF #6, 470
 ESF #7, 470
 ESF #8, 471
 ESF #9, 471
 ESF #5, 551

- ESF #10, 471
 - ESF #11, 471
 - ESF #12, 472
 - Federal partners under ESF #8, 550
 - Emergency Support Team (EST), 470
 - Emerging agents, 323
 - EMS, 2
 - Emulsion systems, 425
 - Encephalitis, 110
 - Encephalomyelitis, 199
 - Encryption, 318
 - Endotoxins, 110
 - Enthalpy of vaporization, 342
 - Environmental biophysics, 121
 - Environmental considerations, 348
 - Environmental factors, 502
 - Environmental Health Laboratory for Chemical Terrorism (EHLCT), 537
 - Environmental Protection Agency (EPA), 345, 517
 - EOC. *See* Department of Health and Human Services
 - Epidemic disease, 534
 - EPidemic Information Exchange System (Epi-X), 545
 - Epidemiology, 122
 - Epidemiology of bioterrorism, 529
 - Epsilon toxin, 199
 - ESF. *See* Emergency Support Function
 - Essential services, 534
 - Ethnically and religiously inspired groups, 35
 - Exanthem, 74
 - Exdetex02, 382
 - Executive Order 12656, 203
 - Exfinder 152, 384
 - Exhaustion, 82
 - Exotoxins, 110
 - Explosions, 55
 - Explosive incident response template, 499
 - Explosives, 23
 - Exposure
 - chemical agents, 373
 - routes of, 347
 - External production signatures, 440
- F
- Fabric filters, 55
 - Fallout, 57
 - False positive, 146
 - Fast atom bombardment mass spectrometry (FABMS), 164
 - FCO, *See* Federal Coordinating Officer
 - Federal agencies, 203
 - Federal Building in Oklahoma City. *See* Oklahoma City bombing
 - Federal Bureau of Investigation, (FBI), 204, 473
 - Hazardous Materials Response Unit), 510
 - response organization, 494
 - Federal Coordinating Officer (FCO), 467, 476, 483, 494, 512
 - Federal disaster response, 467
 - Federal law enforcement assistance, 522
 - Federal On-Scene Coordinator (FOSC), 544
 - Federal Radiological Emergency Response Plan (FRERP), 477, 478, 516, 521
 - Federal Radiological Monitoring and Assessment Center, 268
 - Federal Response Plan (FRP), 465, 467, 489, 491, 528
 - organization of, 490
 - Terrorism Incident Annex, 203
 - Federal support, 223
 - FEMA, 201, 467, 474, 512
 - model, 492
 - Feodossia, 95
 - Fermentation, 109, 111
 - Fertile chicken eggs, 115

- Fiber-optic-based sensor, 148
 - Field ion spectrometry (FIS), 384
 - Fifteenth Directorate, 99
 - Filoviridae, 81
 - Fine mist, 374
 - Finnish M86, 378
 - Fire, 55
 - Firewalls, 318
 - First tier forces, 466
 - Fissile isotopes, 277
 - Fission weapons, 285
 - Flame photometry FPD, 378
 - Flaviviridae, 81
 - Flow cytometry, 158
 - Flow through assay, 172
 - Flowfield, 56
 - Fluorescent aerodynamic particle sizer (FLAPS), 156
 - Fluorescent evanescent wave fiber optic immunosensor, 178
 - Fluorescent particles, 98
 - Fluorochrome fluorescein isothiocyanate (FFI), 158
 - Fogs, 55
 - Food and Drug Administration, 518
 - Food borne transmission, 208
 - Food crops, 121
 - Food supply chain, 123
 - Fort Carillon, 96
 - Fort Detrick, 67, 536
 - Fort Ticonderoga, 96
 - Fouled water, 65
 - Fourier Transform Infra-Red spectroscopy (FTIR), 186
 - FP. *See* Fluorescent particles
 - Francisella tularensis, 76, 109
 - French Indian War, 65
 - French Revolution, 14
 - FRERP. *See* Federal Radiological Emergency Response Plan
 - Frictional force, 52
 - FRP, *See* Federal Response Plan
 - Ft. Douglas, 98
 - Fungi, 125
- G**
- GA nerve gas, 333
 - Gamma-ray spectroscopy, 267
 - Garden sprayer, 104, 376
 - Gas Chromatograph (GC), 380
 - Surface Acoustic Wave (GC/SAW), 392
 - Gastrointestinal, 69
 - GB. *See* Sarin
 - Geiger-Mueller. *See* GM counter
 - Gene splicing, 111
 - General Accounting Office (GAO), 545
 - Generic initial response template, 498
 - Genetic diversity, 137
 - Genetically engineer, 99
 - Genetically modified organisms, 126, 136
 - Geneva Protocol of 1925, 65
 - Genomics, 235
 - Geographic information system, 129
 - Germ warfare, 61
 - Germanium detectors, 267
 - Gilmore Commission, 203
 - GIS (Geographic Information System), 129, 131
 - Glanders, 65, 68, 99, 102, 199
 - GM (Geiger-Mueller) counter, 266, 267
 - GMO (Genetically Modified Organisms), 128
 - Government response, 195
 - Governor's Authorized Representative (GAR), 477
 - GPS (Global Positioning System), 129, 131, 134
 - Gram negative, 76
 - Gravimetry, 57
 - Grey (Gy), 261
 - Gross domestic product, 127
 - Group:
 - activity, 41
 - conflicts, 36

identity, 36
 ideology, 42
 mind, 39
 psychology, 42
 violence, 40
 Guerrilla warfare, 17
 Guidelines for Schedule 1, 327
 Guidelines for Schedule 2, 328
 Guidelines for Schedule 3, 328

H

Hacking, 295
 hack-activism, 294
 Half-life, 259
 Half-value layer (HVL), 261
 Hand held immunochromatographic
 assays (HHA), 171
 Hannibal, 65
 Hantavirus, 69, 110
 Harris Incident, 64
 Hart Rudman Report, 203
 Hazard mitigation site survey teams,
 483
 Hazardous materials (Hazmats), 345
 Baltimore Tunnel fire, 484
 commercially available chemicals,
 435
 teams, 466
 Headache, 82
 Health Alert Network (HAN), 545
 Health physics, 273
 Health services response to a civilian
 chemical attack, 365
 Heat, destruction by, 413
 Hemorrhage, 69
 Hemorrhagic fevers (HF), 61, 199
 symptoms, 81
 treatment, 82
 HEPA (High Efficiency Particulate
 Air) filters, 451, 460
 HgI₂, 267
 HHA, *See* Hand Held immunochro-
 matographic Assays

HHS. *See* Department of Health and
 Human Services, 510
 High explosive chemical vapor
 sensor, 387
 Highly enriched uranium (HEU), 286
 Hiroshima, 24, 278
 HIV. *See* Human immunodeficiency
 virus
 HMD. *See* Hoof and Mouth Disease
 HMRU (FBI's Hazardous Materials
 Response Unit), 510
 Honest John:
 M190, 374
 M79, 374
 Hoof and mouth disease, 124, 128,
 138
 Hospitals:
 first responders, 350
 infection control plans, 223
 preparedness, 539
 skeletal staffing, 222
 Hot Zone, 498
 Howitzer projectiles, 374
 Human biohazard, 104
 Human immunodeficiency virus, 68,
 196
 Human-to-human transmission, 76
 Hydrochlorination, 417
 Hydrogen cyanide, 323, 429
 Hydrogenation, 416

I

ICS, *See* Incident Command System
 ID₅₀, 346
 Identity, 41
 "I Love You" bug, 296
 Immunoassay based identification
 systems, 170
 Immunoassays, 148
 Impaction mechanism, 151
 Impactors, 55
 Incapacitating, 109
 Incapacitating agents, 322

- Incident Command System (ICS),
351, 465, 520, 521, 544
- Incident Commander (IC), 465
- Incineration, 414
- Industrial chemicals, 436
- Infection control, 538
- Infection Control Committee
Chairman, 538
- Infection control officers, 538
- Infectious diseases
emerging, 86
unusual, 536
- Infectious Disease Society of North
America (IDSNA), 536
- Infectious dose, 74, 102
- Information and communication
systems, 122
- Infra red (IR), 386
- InGaAs detector, 147
- Ingestion, 346
- Inhalation anthrax, 70, 102. *See also*
Anthrax
- Inhalation of respiratory secretions,
78
- Inhalational absorption, 346
- Initial actions, 523
- Inoculation of fertile eggs, 109
- Inpatient facilities, 534
- Intensive care, 534
- InterAgency Board for Equipment
Standardization and
InterOperability, 511
- Interferometer biosensor, 182
- Intermediate-Range Nuclear Forces
(INF) Treaty, 289
- Internal production signatures, 440
- International Association of Chiefs of
Police, 465
- International Plant Protection
Convention (IPCC), 128
- International Science and Technology
Center, 289
- International Standards Organization/
Open Systems Interconnect
(ISO/OSI), 304
- International terrorism, 14
- Internet protocol (IP), 307
- Ion mobility detector, 378
- Ion mobility spectrometry (IMS), 383
- Ionization chamber, 267
- Ionizing radiation, 259
- IPCC. *See* International Plant
Protection Convention, 128
- Iran-Iraq war, 432
- Irgun, 19
- Isolation, 129
- Isolation rooms, 534
- Itemiser E, 384
- J
- Jacobin movement, 14
- Japanese encephalitis, 110
- Jewish zealots, 19
- JOC. *See* Joint Operations Center
- Joint Commission on Accreditation of
Healthcare Organizations
(JCAHO), 539
- Joint Information Center (JIC), 475
- Joint Operations Center (JOC), 474,
475, 493
- Joint Service Defense Technology
Objective, 462
- Joint Services Light Integrated Suit
Technology (JSLIST), 456
- Joint Task Force (JTF), 522
Consequence Management (JTF-
CM), 467
JTF-CS, 201, 552
- Junin, 199
- Justice Assistance Act of 1984, 523
- K
- Kaczynski, Theodore, 22, 532
- Kevlar, 461
- Kidney failure, 82

Kosovo, 41
 Kurdish Workers' Party, 19

L

Laboratories, 220, 534
 Lacrimators, 322
 Large-scale fermentation, 114
 Large-scale production, 112
 Laser pyrolysis, 163
 Lassa fever, 81, 99, 199
 Late blight, 97
 LD₅₀, 103, 105, 271, 346
 Lead Federal Agency (LFA), 474, 491, 509, 516
 Leaf blight, 97
 Lethal dose-50. *See* LD₅₀
 Lethal toxin, 69
 Level A protective gear, 350
 Level B laboratories, 536
 Level C laboratories, 536
 Lewisite (L), 326, 357, 459
 LFA. *See* Lead Federal Agency
 LIDAR, 147
 Light detection and ranging, 147
 Light-Addressable Potentiometric Sensor (LAPS), 176
 Line source, 97
 Liquid impingers, 58
 Lisbon Protocol, 289
 Little John (M206), 374
 Little's Law, 313
 Live animals, 109, 116
 Live tissue, 115
 Living organisms, 109
 Local health services, 547
 Local mass transit systems, 235
 Local preparedness, 543
 Local response, 466, 495
 Logic bomb, 301
 Logistical and personnel problems, 368
 Long-term consequences, 364

M

M121A1 GB, 374
 M134 GB, 374
 M139, 374
 M360 GB, 374
 M426 GB, 374
 M687 GB, 374
 Malaria, 196
 MALDI System, 166
 Management of terrorist events
 involving radioactive material, 274
 Management or eradication, 122
 Manhattan Project, 278
 Mapping of the ground
 contamination, 377
 Marburg virus, 68, 99, 110, 199
 Masada, 19
 Mass distribution of emergency medications, 224
 Mass mortalities, handling, 226
 Mass medical care, 221
 Mass spectroscopy (MS), 162, 386
 Matrix Assisted Laser Desorption and Ionization (MALDI), 166
 Matsumoto attack (1994), 530
 Mayak Production Association, 289
 MC1, 374
 McVeigh, Timothy, 22
 Measles, 196
 Mechem Explosive and Drug Detection System (MEDDS), 379
 Medical examiners, 538
 Medical forensic samples, 364
 Medical Response Team (MRT), 367
 Medical services preparedness, 548
 Medieval history, 65
 Merk, George W., 97
 MERS. *See* Mobile Emergency Response Support
 Messina, Sicily, 96

- Metal-Oxide Silicon Field-Effect – Transistor (MOSFET), 397
- Meteorological conditions, 97
- Metropolitan Medical Response System (MMRS), 230, 367, 518, 542
- Microbial content, 149
- Microbial identification systems, 536
- Microbiology, 61
- Military, role of, 201
- Military grade weapon, 63
- Military support, 521
- Millimeter electromagnetic wave (MEW), 392
- Mines, 374
- Ministry of Agriculture, 99
- Ministry of Defense, 99
- Ministry of Health, 99
- Milosevic, Slobodan, 41
- Ministry of Medical and Microbiological Industries, 99
- Missile, 98, 99
- Mission, type of, 448
- Mission Oriented Protective Posture (MOPP), 456
- Mists, 55
- MK116, 374
- MO2, 384
- Mobile Emergency Response Support (MERS), 479, 523
- Mobile Operations Center (MOC), 479
- MOC, 523
- Molecular excitation, 156
- Molecular transformations, 134
- Molecular weight, 340
- Molten metal systems, 415
- Monkeypox, 74, 99, 110
- Morality and conscience, 42
- Morgue facilities, 534
- Mortar shell, 374
- Mouth and throat, 74
- MSI, 134
- Mucosa, 74
- Multiple sensor integration, 134
- Multisensor data fusion, 134
- Munitions, 24, 96, 98
- Muscle aches, 82
- Mustard, 333
- Mustard gas, 323, 429
- Mycoplasmas, 125
- Mycotoxins, 110
- Mycoplasma, 109
- N
- Nagasaki, 24, 278
- National Animal Health Reporting System (NAHRS), 122
- National Association of Clinical Laboratory Scientists (NACLS), 536
- National Center for Super Computer Applications, 300
- National Contingency Plan, 521
- National Council on Radiation Protection and Measurements (NCRP), 274
- National Disaster Medical System (NDMS), 224, 468, 518
- National Domestic Preparedness Office (NDPO), 512, 535
- National Emergency Coordination Center (NECC), 367, 479
- National expertise, 535
- National Fire Academy (NFA), 345, 465
- National Fire Protection Association (NFPA), 458
- National Guard, 522
- Civil Support Teams (CSTs), 515
- National Institute of Allergy and Infectious Diseases (NIAID), 234
- National Institutes of Health, 233

- National Institute of Occupational Safety and Health (NIOSH), 455
- National Laboratory Training Network (NLTN), 536
- National Medical Chemical and Biological Advisory Team, 514
- National Medical Response Teams (NMRS), 224
- National Office for Combating Terrorism, 2
- National Oil and Hazardous Substances Pollution Contingency Plan, 517
- National Plant Board (NPB), 133
- National Response Plan, 366
- National Security and Emergency Preparedness (NS/EP), 469
- National Security Council (NSC), 527
- National Security Presidential Directive-1, 204
- National security strategy, 515
- Nd:YAG Laser, 157
- Necrosis, 69
- Nematodes, 125
- Nerve agents, 322
- Nerve gas, 24
- Network delays, 309
- Network Interface Card (NIC), 306
- Neurotoxins, 84, 110
- Neutralization, 416
- Neutron, 277
 - detectors, 267
 - multiplication Factor, 279
- Neutron-based detection systems, 398
- NGOs, 529
- Nipah virus, 69
- Nitrile gloves, 505
- Nitroglycerin, 23
- NLRN, 537
- Nomex, 461
- Non-Proliferation Treaty, 288
- Non-specific detection, 156
- No-tag biosensors, 180
- NPB. *See* National Plant Board
- Nuclear expertise and materials, protection of, 290
- Nuclear explosions, 48, 55
- Nuclear infrastructure, destruction of, 290
- Nuclear installations, 287
 - sabotaging of, 285
- Nuclear Magnetic Resonance (NMR), 391
- Nuclear threats, terrorism, 285
 - response to, 267
- Nuclear weapons, 24, 277
- Nucleation, 55
- Nucleic acid-based identification systems, 168
- O
- Observations, 376
- Occupational Health and Safety Administration (OSHA), 448
- Office International des Epizooties, 128
- Office of Emergency Preparedness (OEP), 201, 224, 542
- Office of Homeland Security, 203
- Office of National Preparedness (ONP), 528
- Offsite Consequence Analysis (OCA), 435
- OIE. *See* Office International des Epizooties
- Oil supplies, 127
- Oklahoma City bombing, 6, 7, 22, 322
- Olympic Games, Atlanta bombing, 4
- On-Scene Commander (OSC), 474
- Operation Whitecoat, 67
- Optical fiber sensors (OFS), 390
- Optical methods, 378
- Organization of rescue, 351
- Orthopoxvirus, 74

Ortho-Chlorobenzylidene-
Malononitrile (CS), 326
Outbreak investigation, 218

P

- Packet order, 303
Pahlavi, Shah, 19
Palestinian attacks, 17
Palytoxin, 110
Pandemics, 78, 544
Papules, 74
Paranoia, 42
Parasites, 125
Particles, 47
 concentration, 49
 mobility, 51
 sizes, 49
Password system, 317
PCR. *See* Polymerase Chain Reaction
PDD-39. *See* Presidential Decision
 Directive 39
Penetrating agents, 322
Persian Gulf War, 24, 145
Personal Device Assistants (PDA),
 300
Pesticides, 55
Petechiae, 82
Pharmaceutical production, 117
Pharmaceutical supplies, 534
Phi-X174 bacteriophage, 460
Phosgene, 323, 346, 429
Phosgene oxime, 357
Photomultiplier, 156
Psychology of terrorist acts, 37
Physician preparedness, 535
Picric acid, 23
Piezoelectric biosensor, 183
Piezoelectric crystal balance, 182
Pine Bluff, Arkansas, 97
Plague, 61, 68, 78, 99, 109, 199, 209,
 536. *See also* Bubonic plague,
 Pneumonic plague
 incubation, 80
 symptoms, 78
 treatment, 79
Planning assumptions, 520
Plants:
 diseases, 124
 growth inhibitors, 322
 pathogens, 97
 pathology, 124
 protection and quarantine, 122
Plasma-based destruction, 415
Plastic explosives, 383
Plumes, 55
Plutonium, 286
 Pu-239, 277
Pneumonic plague, 78, 79, 102
Pneumonic tularemia, 77. *See also*
 Tularemia
Point detection, 149
Point source, 97
Polarization, 37
Polio, 196
Political effects, 14
 strategic, 16
Polonium, 282
Polymerase Chain Reaction (PCR),
 130, 169
Polymer-based garments, 457
Polypeptides, 110
Portability, 378
Portable biofluoro-sensor (PBS), 160
Portable digital lidar (PDL), 148
Portable isotopic neutron
 spectroscopy (PINS), 400
Post traumatic stress disorder (PTSD),
 226
Postexposure protocols, 538
Powered air-purifying respirators
 (PAPRs), 453
Pox, 74
PPQ (Plant Protection and
 Quarantine Unit, APHIS), 122
Precursors, 330
Preemption, 206

- Presidential Decision Directive 39
 (PDD-39), 203, 473, 491, 509,
 534
 Presidential Decision Directive 62,
 515
 Primary aerosol, 58, 101
 Primary unit, 99
 Prioritization of vaccine recipients,
 225
 Projectiles, 374
 Projective identification, 38
 Proliferation, 100
 ProMED, 214, 233, 248
 Property damage, 489
 Prophylactic drug treatment, 538
 Proportional counters, 267
 Protection of first responders, 350
 Protective clothing
 battle dress over-garments (BDO),
 456
 chemically protective, 456, 457
 liquid splash-protective, 457
 thermal, 461
 undergarments, 456
 Protective equipment, personal (PPE),
 447
 need vs. availability, 449
 selection of the most appropriate,
 449
 Protective materials, 462
 Protein interactions, 134
 Proteins, 110
 Protocol for notification, 540
 Protozoa, 125
 Provisional Irish Republican Army,
 17, 19
 Psychological and economic
 terrorism, 125
 Psychological distress, 226
 Psychological ramifications, 232
 Psychotomimetic agents, 359
 Public information, 229
 Pulsed fast neutron analysis (PFNA),
 401
 Pustules, 74
 Pyrolysis, 415
- Q
- Q Fever, 99, 102, 110, 199
 Q-DLTS. *See* Charged based deep
 level transient spectroscopy
 QNB (agent BZ), 326
 Quartz crystal microbalance (QCM),
 393
 Queuing, 309
- R
- R-400 Bomb, 100
 Radiation
 detection, 265, 273
 dose, 269
 effect of, 270
 exposure, 261
 shielding, 260
 Radioactive Particles, 48, 54
 Radiological Assessment Program,
 268
 Radiological Assistance Program
 (RAP), 467
 Radiological incident template, 505
 Radiological protection, 460
 Raman scattering (RS), 388
 Rand Report, 1
 Rapid diagnostic, 129
 Rapid prototyping system, 135
 Rapid Response Information System
 (RRIS), 482
 RAPTOR, 180
 RDT&E, 2
 RDX, 383
 Recession, 127
 Reconstruction Information Center
 (RIC), 481
 Red bumps, 74
 Regional Operations Center (ROC),
 470, 476
 Regional planning, 223

- Reign of Terror, 23
Release and transmission, 206
 other, 210
Remote sensing, 130
 technology, 131
Reporting a suspected bioterrorism
 event, 539
Reporting and inspection
 requirements, 442
Republic of Texas, 8
Research and development signatures,
 439
Research needs, 232
Resonant mirror biosensor, 184
Respirator designs, 455
Respirator protection, 429
Respiratory protection equipment,
 451
Respiratory tracts, 49
Respiratory ventilation facilities, 534
Response and recovery actions, 523
Response, recovery & mitigation
 actions, 521
Resuspension, 56
Ribavirin, 82
Rice blast, 97
Ricin, 102, 110, 174, 199, 359
Rickettsiae, 98, 110
Rift Valley fever, 81, 110
Rinderpest, 124
Risk assessments, 133, 432
 techniques, 448
RNA, 110
 expression, 134
 viruses, 81
Rodent population, 78
Roentgen, 261
Rogue states, 432
RSA encryption system, 319
- S
- Safe distance from an explosive
 device, 500
Salmonella, 109
Salmonella typhimurium, 65
SALT. *See* Strategic Arms Limitation
 Talks
SALT II Treaty, 288
Samonella typhi, 109
Sampling devices, 149
Sarin (GB), 6, 24, 333, 459, 530
SAS statistics package, 133
Satellite, 132
Saxitoxin, 110, 359
Scapegoating, 42
Scintillation detectors, 267
Sea dumping, 413
Second tier forces, 466
Second generation FLAPS, 157
Secondary cases, 75
Secondary devices, 499
Secondary transmission, 211
Secure locations, 62
Self-contained breathing apparatus
 (SCBA), 350, 454
SEMA (State Emergency
 Management Agency), 544
Sensitive membrane antigen rapid
 test, 145
Sensitivity, 378
September 11, 2001, 9, 123, 126, 127,
 136
Sequence-tagged sites, 130
Sergeant (M212), 374
Serratia marscens, 97
Service time, 310
SHADY GROVE project, 99
Shared experience, 36
Shell, 99, 374
Shortage in the medical field, 222
Sievert (Sv), 261
Sikh nationalist, 19
Single nucleotide polymorphism, 130
Single particle fluorescent analyzer
 (SPFA), 157
Skin rash, 74
SM. *See* Serratia Marscens

- Small scale fermentation, 114
 Smallpox, 61, 65, 74, 96, 99, 102, 104, 198
 diagnosis, 74
 incubation, 74
 in New York City - 1947, 75
 symptoms, 74
 treatment, 75
 vaccination, 75, 104
 weapon form, 76
 Small-scale deployment, 104, 375
 Small-scale use of live animals, 116
 Small-scale use of live tissue, 116
 Small-scale weapon, 435
 SMART tickets, 145, 173
 Snake venom, 110
 SNP (single nucleotide polymorphism), 130
 Society for Microbiology, 536
 Software threats, 301
 Soil sterilants, 322
 Sore throat, 82
 Soros Foundation, 289
 Soviet Union, 66, 68
 Spatial-temporal analysis, 121
 Spectroscopic methods, 186
 Spider venom, 110
 S-PLUS, 133
 SPR (surface plasmon resonance), 180, 181
 Spray, 374
 Sprayers, 55, 100, 374
 SPSS statistics package, 133
 Stafford Act, 467
 Stafford Disaster Relief and Emergency Assistance Act, 507
 Staging area, 499
 Standard analysis of variance, 133
 Stand-off detection system, 147
 Staph enterotoxin, 174
 Staphylococcal, 359
 Staphylococcal enterotoxin B, 102, 199
 StarLink, 137
 START I treaty, 289
 START II, 289
 START III, 290
 State and local governments, 204
 State Coordinating Officer (SCO), 467
 State Department of Health, 543
 State Public Health Service preparedness, 543
 State response, 466. *See also* SEMA
 Stem rust, 97
 Stemutators, 322
 Stimson, Henry L., 97
 Stockholm International Peace Research Institute, 35
 Stockpile stewardship, 290
 Strategic Arms Limitation Talks (SALT), 288
 Strategic Information and Operations Center (SIOC), 474
 Strategic weapons, 95
 Streptavidin-enzyme complex, 169
 STS (sequence-tagged sites), 130
 Submunitions, 99, 374
 Suborbital, 132
 Super-computing clusters, 300
 Supercritical water oxidation and wet air oxidation, 415
 Supreme truth, 6
 Surface acoustic wave (SAW), 392
 Surface distributions, 49
 Surface plasmon resonance. *See* SPR
 Surface wipes (SW), 401
 Surveillance for bioterrorism, 213
 Sverdlovsk, 11, 71
 Syndromic surveillance, 214
 Syphilis, 214
 Systemic poisons, 322
- T
- T-2 mycotoxins, 102
 Tabun, 323

- Tandem mass spectrometer (TMS), 386
 - Tanks, 24
 - Targeting at the molecular level, 167
 - Tartars, 65, 95
 - Taylor Cone, 165
 - TCP/IP, 304
 - Tear agents, 322
 - Technical support working group, 233
 - Technology
 - in agroeconomic terrorism, 129
 - available, 451
 - terrorism and, 22
 - of transport, 24
 - up-converting phosphor, 185
 - Telecommunications service priority (TSP), 469
 - Teleregistration, 483
 - Temorgens, 110
 - Terrorism
 - definition of, 14
 - deterrence of, 21, 205
 - face of, 36
 - political violence and, 14
 - psychology of, 36
 - psychological and economic, 125
 - response, 202
 - Terrorist events, 5
 - Tetracycline, 79
 - Tetrodotoxin, 110
 - Thermal neutron activation, 399
 - Thermonuclear weapon, 279
 - Thermo-Redox (TR), 394
 - Third tier forces, 467
 - Thorium-Th-233, 277
 - Three Mile Island (TMI), 272, 487
 - Tier I, 496
 - Tier II, 497
 - Tier III, 497
 - Tier IV, 496
 - Time-Phased Force and Deployment List (TPFDL), 481
 - Tissue, 109
 - Tissue-injuring agents, 356
 - Title 10 authority, 523
 - TNT, 23, 383
 - Tokyo subway attack (1995), 6, 24, 530
 - TOPOFF exercise, 228, 485, 548
 - Top-soil, removal of, 424
 - Totalistic belief systems, 42
 - Toxic chemicals, 329, 345
 - destruction of, 412
 - Toxic industrial chemicals (TICs), 459
 - Toxic industrial materials (TIMs), 459
 - Toxics release inventory (TRI), 435
 - Toxin agents, 359
 - Toxins, 61, 109, 110, 359
 - Traffic control, 498
 - Training, 229
 - for the general public, 231
 - Trapdoor, 301
 - Trinitrotoluene, 23
 - TriPropylAmine (TPA), 174
 - Trojan horse, 301
 - TSH antibody, 174
 - Tuberculosis, 196
 - Tularemia, 61, 68, 97, 99, 102, 109, 174, 199, 536
 - incubation, 77
 - symptoms, 76
 - treatment, 77
 - typhoidal, 77
 - Typhus, 199
- U
- U.S. Army Corps of Engineers (USACE), 522
 - U.S. Army Soldier Biological Chemical Command (SBCCOM), 107, 461
 - U.S. Marine Corps Chemical Biological Incident Response Force, 146
 - U.S. Policy on Counterterrorism, 473

- U.S.-Russia Strategic Offensive
 Reductions Treaty, 290
 Ulceroglandular, 77
 Ultra violet (UV), 386

 Ultra violet laser-induced
 fluorescence (UV LIF), 147,
 157
 Unabomber. *See* Kaczinski, Theodore
 Unified command system, 465
 Unit 731, 97
 United Nations Special Commission,
 73
 UNIX system, 317
 Unmanned aerial vehicle (UAV), 148
 Upgrade intelligence programs, 290
 Uranium, 285
 U-235, 277
 Urban Search and Rescue (US&R),
 481
 US Army Chemical Warfare Service,
 67
 US Army Medical Research Institute
 for Infectious Diseases. *See*
 USAMRIID
 USAHA (US Animal Health
 Association), 122
 USAMRICD (US Army Medical
 Research Institute for
 Chemical Defense), 514
 USAMRIID (US Army Medical
 Research Institute for
 Infectious Diseases), 67, 201,
 514, 519, 536
 USDA, 122
 U.S. government, role of, 200
 USS Cole, 7
 USSR, 66, 68
 BW program, 99

 V
 Vaccination, 233, 538
 manufacture, 197

 Vaccinia, 74
 Vapor pressure, 341
 Variola major, 74
 Variola minor, 74
 Vendor managed inventory (VMI),
 552
 Venezuelan equine encephalitis, 102,
 110
 Venezuelan HF, 81
 Ventilation system, 56
 Verification and identification of
 agents, 376
 Vesicants, 322
 Vesicating (blistering) agents, 356
 Veterinary Services Unit (VS), 122
 Viable particle-size impactors, 150
 Vibrio cholerae, 109
 Vice President's task force, 3
 Vietnam War, 65
 Violence against plant, animal or
 human, 125
 Viral agents, 110
 Viral hemorrhagic fever, 80, 102, 110
 Viral production process, 115
 Virions, 81
 Virtual impactors, 150, 152
 Virus, 109, 125
 transmission of, 75
 Volatility, 341
 Volcanic eruptions, 55
 Vomiting agents, 322
 Vulnerabilities, 123
 VX nerve agent, symptoms, 353

 W
 War Reserve Service, 97
 Warhead, 374
 Waterborne transmission, 207
 Weaponization, 72, 73, 96, 99
 Weapons of mass destruction
 (WMD), 62, 197, 495
 management of an event, 493
 WMD Operations Unit, 510

Weapons tests, 57
West Nile disease, 110, 209
Western equine encephalitis, 110
White pox, 110
Who are terrorists, 18
Why terrorism, 16
WMD. *See* Weapons of Mass
Destruction
Working Group on Civilian
Biodefense, 77
Workstation security, 295
World Health Organization, 74, 214
World Organization for Animal
Health, 128
World Trade Center (WTC) bombing
(1993), 5
World War I, 96
World War II, 24, 65, 96
World Wide Web, 27
Worm, 301
WTC. *See* World Trade Center (1993)
and September 11, 2001

X

XM-2 air samplers, 145
XM736 VX, 374
X-rays, 265, 397
analysis of x-ray detection, 398

Y

Yellow fever, 81, 110
Yellow rain, 110
Yersinia pestis, 78, 109, 174

Z

Zealots, 23
Zoonotic and agricultural
transmission, 209
Zoonotic diseases, 209