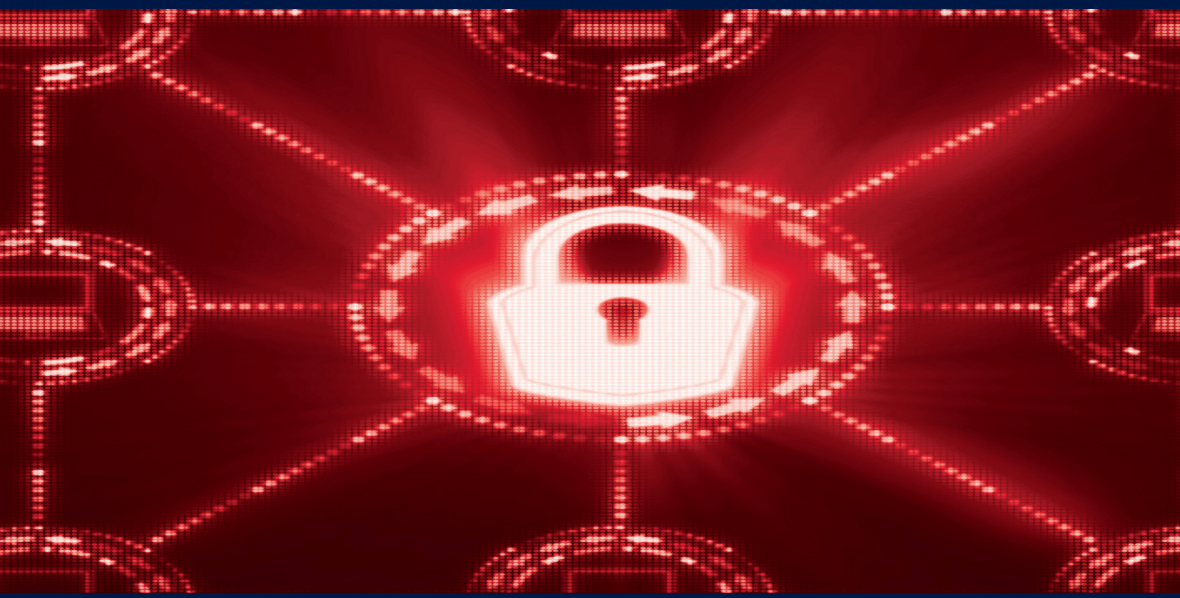
INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES



Chinese Cybersecurity and Defense

Edited by Daniel Ventre

ISTE WILEY

Chinese Cybersecurity and Defense

Chinese Cybersecurity and Defense

Edited by

Daniel Ventre

ISTE

WILEY

First published 2014 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2014941991

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-614-3

Printed and bound in Great Britain by CPI Group (UK) Ltd., Croydon, Surrey CR0 4YY

Contents

Author Biographies

Dean Cheng is the Senior Research Fellow for Chinese political and security affairs at the Asia Studies Center of The Heritage Foundation. He specializes in Chinese military and foreign policy, and has written extensively on Chinese military doctrine, technological implications of its space program, and "dual use" issues associated with China's industrial and scientific infrastructure.

Before joining The Heritage Foundation, he was a senior analyst with the Center for Naval Analyses, a federally funded research and development center, and a senior analyst with Science Applications International Corporation (SAIC), the Fortune 500 specialist in defense and homeland security. He has testified before Congress, spoken at the (American) National Defense University, US Air Force Academy, and the National Space Symposium, and been published in the Wall Street Journal and the Washington Post.

Alan Chong is Associate Professor at the S. Rajaratnam School of International Studies in Singapore. He has published widely on the notion of soft power and the role of ideas in constructing the international relations of Singapore and Asia. His publications have appeared in *The Pacific Review*; *International Relations of the Asia-Pacific*; *Asian*

Survey; *East Asia: an International Quarterly*; *Politics, Religion and Ideology*; the *Review of International Studies*; the *Cambridge Review of International Affairs* and *Armed Forces and Society*. He is also the author of *Foreign Policy in Global Information Space: Actualizing Soft Power* (Palgrave, 2007). He is currently working on several projects exploring the notion of 'Asian international theory'. His interest in soft power has also led to inquiry into the sociological and philosophical foundations of international communication. In the latter area, he is currently working on a manuscript titled 'The International Politics of Communication: Representing Community in a Globalizing World'. In tandem, he has pursued a fledgling interest in researching cyber security issues. He has frequently been interviewed in the Asian media and consulted in think-tank networks in the region.

Alice Ekman is Associate Research Fellow in charge of China at the French Institute of International Relations (Ifri), where she conducts analyses of major domestic and foreign policy developments. She is an Adjunct Professor at Sciences Po in Paris, and also lectures at the French Institute for Higher National Defense Studies and the War College. Alice Ekman was formerly Visiting Scholar at Tsinghua University (Beijing), Research Officer at the Embassy of France in China, and Consultant in a Paris-based strategy firm. Fluent in Mandarin Chinese, she regularly undertakes research fieldwork in China and East Asia.

She holds an MA from the London School of Economics in International Relations, Economics, and Anthropology (China focus), and a PhD in International Relations from Sciences Po. Alice Ekman is currently a member of the EU committee of the Council for Security Cooperation in the Asia Pacific (CSCAP).

Thomas Flichy de La Neuville is Professor in international relations at Saint-Cyr military academy. Specialist of Iran, he has studied persian in the National Institute of Oriental Languages an cultures and holds a PhD in legal history. He is visiting professor in Oxford and Annapolis. Amongst his recent publications, *Iran-Russia-China, a new mongol empire?*

Xu Longdi is a PhD and Associate Research Fellow at China Institute of International Studies (CIIS), Beijing. He received his PhD in international relations from the Graduate School of the Chinese Academy of Social Sciences (CASS) in 2009 and joined CIIS the same year. His expertise covers International Relations Theory, international security, and EU politics and foreign policy. Now he runs a program on "International Norms and Cyber Security".

Samuel Cherian is Associate Fellow in the Strategic Technologies Centre at the Institute for Defence Studies and Analysis, an autonomous think tank affiliated to the Indian Ministry of Defence. He has written on various cyber security issues, including critical infrastructure protection, cyber resilience, cybercrime, and internet governance. He has also presented on these topics at seminars and round tables around the world as well as different fora in India. His recent publications include *Cybersecurity and Cyberwar*, (October 2013 issue of *Seminar* magazine), *Emerging Trends in Cyber Security*, (IDSA Web Comments March 28, 2012), and *Prospects for India-US Cyber Security Cooperation*, (Volume 31, Issue 2, Strategic Analysis September 2011). His monograph *Global, Regional and Domestic Dynamics of Cybersecurity* will be published shortly. He was co-ordinator of the IDSA Task Force on Cyber Security which published a report on "*India's Cyber Security Challenges*" in March 2012.

He holds a PhD from the Jawaharlal Nehru University, New Delhi.

Daniel Ventre holds a PhD in Political Science (University of Versailles). He is the Secretary General of GERN (*Groupe Européen de Recherches sur les Normativités – European Research Group into Norms*), researcher at CESDIP (*Center for Sociological Research on Law and Criminal Justice Institutions. CNRS / University of Versailles / Ministry of Justice*), Chairholder in Cyber Security & Cyber Defense (*Saint-Cyr / Sogeti / Thales*). He is the author of a number of books and articles (published in French, English and Chinese) on cyberwarfare, information warfare, cyberconflict, cybersecurity and cyberdefense. He has published:

Information Warfare – 信息战, National Defense Industry Press, Beijing, 218 pages, January 2014.
Cyber Conflicts, Competing National Perspectives, ISTE, London and John Wiley & Sons, New York, May 2012, 330 pages.
Cyberwar and Information Warfare, ISTE, London and John Wiley & Sons, New York, July 2011, 448 pages.
Cyberattaque et Cyberdéfense, Paris, Editions Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", August 2011, 312 pages.
Cyberespace et acteurs du cyberconflit, Paris, Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", April 2011, 288 pages.
Cyberguerre et guerre de l'information. Stratégies, règles, enjeux, Paris, Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", September 2010, 318 pages.
Information Warfare, ISTE, London and John Wiley & Sons, New York, 2009, 298 pages.
La guerre de l'information, Paris, Hermès Lavoisier, Collection "Finance Gestion Management", 2007.

Introduction

Regardless of the origins of cyberspace (those who designed it, the founding fathers of computing, of telecoms, of the Internet, the first to give financial backing to these projects, etc.), what is important to look at in today's world is the current configuration of cyberspace, and its possible future. Whilst a map of the under-sea cable networks shows the Internet as being rather US-centered, or at least organized around the triad of the USA, Europe and Asia, with the other regions of the world appearing to lie on the periphery, this centrality of infrastructures (root name servers, computation capacities, data flux, etc.), but also of investment, research, users, etc., is in the full throes of evolution. Technology and knowledge are now being disseminated throughout the world. Where it is impossible to install hardwired technologies quickly enough, mobile telephony is becoming an important means of access to the Internet. Poorer populations are beginning to gain access to a Web connection. Thus, modern technologies are able to make their effects felt even in territories where they are not as omnipresent as in the United States. The technology is becoming more widely available, and we can see that the barriers to development are not economic or technical, but often political: the development of cyberspace, and the form

Introduction written by Daniel VENTRE.

that it takes, are subject to the will of the political authorities.

Whilst the United States still seem, at present, to be the dominant force in terms of the Internet and cyberspace, the more widely the technology propagates, the less the number of users is concentrated in the Western World. This evolution of cyberspace is contributing to the current shift of power (economic, political and strategic power) from America toward Asia. The report "The World in 2025"[1] affirms (and it is not alone in doing so) that "the centre of gravity of world production will move towards Asia [...] Before 2025 China could become the second world economic power". This shift is not solely economic. It runs deeper, corresponding to the shifting of the very foundations of the power of modern nations: "*Before 2025 China could become the second world economic power [...] India and China could thus account for approximately 20% of the world's R&D*". The configuration of cyberspace is constantly changing as well. There is no truly stable balance. The same report highlights the effects this evolution will inevitably have: "*If the United States remain the first military power, the scientific and technological catching-up of some states, the new irregular war tactics and the increasing importance of cyber-attacks will weaken their freedom of action*".

Although, evidently, the domination of cyberspace (particularly in economic, political and military terms) depends on more factors than simply the number of users in a state (there are other variables determining the power balance in cyberspace: political goals, industrial expertise, capital, knowledge, data, infrastructure, the capacity to impose a strategy on all three levels of cyberspace), the evolution of uses and populations of users represents a major phenomenon,

1 European Commission, *The World in 2025. Rising Asia and Socio-Ecological Transition*, Brussels, 2009, 28 pages, [http://ec.europa.eu/research/social-sciences/pdf/the-world-in-2025-report_en.pdf].

because it also reflects the changing desires, political, economic and ideological projects. This evolution reflects, or perhaps heralds, a gradual transfer of power from one center (the United States) to another (China). China is, without a doubt, the major player in this reconfiguration. The stakes are enormously high, because if, tomorrow, the 1.5 billion Chinese were all to have access to the Internet, the configuration of China's cyberspace itself and of the world as a whole, would be turned on its head. In cyberspace, Asia is becoming the most important resource in terms of users, consumers, citizens, but also (potentially at least) of creators, designers, although innovation in these domains appears, as yet, to be concentrated in Silicon Valley and in Israel (notably in the domain of cybersecurity). The center of innovation, in the field of ICTs, could, in time, be shifted from America, with its giants of industry and research, to Asia. Even at this stage, China has already developed its own solutions – alternatives to the tools employed in the West (Facebook, Twitter, operating systems, etc.), and its industrial players (e.g. Huawei and Lenovo) are in the process of dethroning the historical international market leaders. By exporting its technologies, and investing in the development of infrastructure in developing countries, China is also creating the conditions for future dependency on its technologies. No doubt China will also be able to invest wisely in technologies with a promising future – e.g. those which will feed into the up-and-coming "Internet of Things" – firstly because of its immense national market, but also because engineers, who are already digital natives, constitute a potential creative resource. In addition, a billion or more Chinese citizens in cyberspace also represent phenomenal quantities of data produced. It is a crucial focal point for authorities, companies and even states to be able to cope with these amounts of data. The capacities to innovate, invest and deploy one's technologies throughout the world constitute as many variables of importance for the power of modern states. Asia, and particularly China, intends to play the leading roles in these domains.

When thinking about the issues of cyberspace, its influence on the quality of international relations and on the evolution of the world, and looking at the importance of cyber strategies for national and international equilibria, China is naturally at the center of the debate. The questions are numerous: what are the variables affecting Chinese power? What is China's ambition – what role does it hope to play on the international stage? In what ways can its society and its political regime evolve? How does cyberspace fit in with these issues of both internal and international politics? What will be the consequences of the evolution of cyberspace and of its use, for Chinese society, for other countries in the region, and for the rest of the world? Are the proposals formulated and the initiatives taken by China in terms of governance of the Internet able to reshape the interconnection of the world such as it is imagined and defined by the West? The evolution of cyberspace, with the central role that China now plays and will continue to play for a long time to come, is now a matter of security and national defense. Cybersecurity and cyberdefense are political and strategic issues of prime importance. Practices, intentions and projects in this field have a direct influence on international relations. New actors, new forms of relations between states, new powers, conflicts and power distributions are taking shape throughout cyberspace.

The aim of this book is to analyze China's policies, strategies and practices in the area of cybersecurity and cyberdefense; and also to analyze the effect they have on the political and strategic choices made by other states. Contributions to this work have come from seven researchers, specializing in international relations and issues of cybersecurity. The individual chapters are drawn from a conference which took place in Paris, on 1 July 2013, organized by the *Chair of Cyberdefense and Cybersecurity* (Saint-Cyr / Sogeti / Thales).

1

China's Internet Development and Cybersecurity – Policies and Practices

1.1. Introduction

After land, sea, air and outer space, many people have dubbed cyberspace as the fifth domain for human activities, with multiple implications for a state. Put simply, the political, economic and security interests of a state are now increasingly connected with cybersecurity. However, the Internet is a double-edged sword, i.e. it brings about not only enormous benefits but also numerous risks, challenges and threats. Therefore, given the borderless, transnational and unique nature of cyberspace, it has become a new frontier for global governance.

China attaches great importance to Internet development and has made enormous progress in this regard. However, as a late comer to this field, China faces various challenges and has been one of the major victims of cyber-attacks. Looking into the future, China is willing to strive for a peaceful, secure, open and cooperative cyberspace together with the international community.

Chapter written by Xu LONGDI.

Internationally, there are many doubts about China's policies and practices in its Internet development because of misunderstanding, prejudice, lack of knowledge, and even ignorance one the one hand. On the other hand, there is an increasing demand for understanding China's policies and practices in this domain. This chapter tries to introduce some of China's cyber policies and practices with a view to mitigating the doubts towards China.

This chapter is divided into six sections: the first section presents an overview of the development of Internet in China; the second section introduces China's policies towards Internet development; the third section elaborates on the cyber legislation and Internet administration in China; the fourth section examines China's idea on cyber diplomacy and its relevant activities and international cooperation concerning the Internet; the fifth section explores whether there is a cyberstrategy in China and its possible shape in the future. Finally, this chapter draws some temporary conclusions in line with the above analysis.

1.2. Internet development in China: an overview

Although China came relatively late to the Internet, the Chinese government and people warmly greeted the advent of the Internet era. During the mid- and late-1980s, China's researchers and scholars began to explore in an active manner the use of the Internet with the assistance of their foreign colleagues. On such occasions as the 1992 and 1993 INET annual conferences, Chinese computer specialists asked for Internet access for the Chinese public as a whole, which gained the understanding of and support from their international peers. During the China-U.S. Joint Committee of Science and Technology Cooperation meeting held in Washington in April 1994, the Chinese representatives ultimately reached a consensus with the U.S. National Science Foundation (NSF) on China's access to the Internet.

On 20 April 1994, the CAINONET for Education and Scientific Research in Zhongguancun district, Beijing was linked to the Internet via a 64k special line. This full-function connection marked China's formal access to the Internet.[1]

Since its inception in China, the Internet has witnessed a rapid and sound development. As of the end of December 2013, the number of Internet users in China has reached 618 million, a growth of 53.58 million over the end of 2012, according to the *33rd Statistical Report on Internet Development in China*[2] released by China Internet Network Information Center (CNNIC) in January 2014. The Internet penetration rate is 45.8%, a growth of 3.7% compared with that at the end of 2012. This figure indicates that the growth rate of the overall scale of Internet users in China has gradually slowed down since 2011.

In the meantime, the number of mobile Internet users has also experienced rapid growth. By the end of 2013, China had 500 million mobile Internet users, a growth of 80.09 million compared with that of 2012 and an annual growth rate of 19.1%. Among all the Internet users, the proportion of those using mobile phones to access the Internet rose from 74.5% to 81.0%, up by 6.5% over 2012. Mobile phones constituted the largest Inter-accessing terminal for the Chinese Internet users. The ratio of Internet users using desktops and laptops dropped slightly to 69.7% and 44.1% by 0.8% and 1.8% respectively, compared with the figure of 2012.

1 State Council Information Office, *White Paper on the Status of China's Internet*, 8 June 2010; 国务院新闻办公室：《中国互联网状况》白皮书，2010年6月8日。http://www.scio.gov.cn/zfbps/ndhf/2010/201006/t662572.htm.

2 China Internet Network Information Center (CNNIC), *The 33rd Statistical Report on Internet Development in China*, January 2014; 中国互联网络信息中心：《第33次中国互联网络发展状况统计报告》，2014年1月。http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201403/P020140305346585959798.pdf.

The rural Internet users had accounted for 28.6% of the total in China, reaching 177 million, a growth of 21.01 million over 2012.

China had a total of 18.44 million domain names, which included 10.83 million ".CN" domain names, up by 44.2% compared with that of 2012, accounting for 58.7% of the total domain names in China.

The total number of websites in China rose to 3.20 million, a growth of 520,000, up by 19.4% compared with that of 2012.

As of the end of 2013, 93.1% of Chinese enterprises use computers in their work, 83.2% use the Internet, 79.6% use broadband. In the meanwhile, the proportion of online marketing and online purchase conducted by the Chinese companies was 23.5% and 26.8% respectively, while that of using the Internet to conduct marketing and advertisement activities was 20.9%.

Along with the gradual slowing-down of the growth rate of the overall scale of the Chinese Internet users, the Internet in China is changing from a quantity-focused development model to a quality-focused one. In other words, the main thematic mission of the Internet in China has shifted from "increasing its penetration rate to deepening its utilization levels", which results from several factors, including changes in the policy environment. For instance, there has been increasing national policy support. In 2013, the State Council issued a policy paper "Opinions on Promoting Information Consumption to Expand Domestic Demand", which demonstrates the importance of the Internet in the Chinese economy and society. Moreover, the Internet is increasingly connected with traditional economy, for instance, it has witnessed very good applications in shopping, logistics, payment, and even finance. Furthermore,

the use of the Internet is gradually changing people's lifestyle, exerting influence upon almost every aspect of their daily life, including clothing, food, housing and transportation, and so on.

Of course, the development, spread and application of Internet in China also face various problems, such as regional imbalance as well as that between urban and rural areas. Constrained by such elements as economic development, education and overall level of social Informationization, China's Internet also takes on a unique feature, i.e. the Eastern part of China enjoys rapid Internet development while that of the Western part is slow, and the urban Internet penetration is high while that in the rural area is low. As of the end of 2009, Internet penetration in the Eastern part of China was 40.0%, while that of the Western part was 21.5%. In addition, there is also a big gap between urban and rural netizens, though the proportion of the latter has witnessed some increase from 27.8% in 2009 to 28.6% in 2013. Therefore, China still needs to make assiduous efforts to narrow the gap between different regions as well as that between urban and rural areas. The Chinese government will have to continue to promote Internet development and spread, thus making more people benefit from it.

1.3. China's policies towards Internet development

China sees Internet as a major opportunity for its reform, opening-up, and modernization cause. The Chinese government has formulated a series of policies, which map out the blueprints for its Internet development, clarify the priorities for different stages of Internet development, and promote the process of social informationization.

1.3.1. *From the very beginning of its development, China's Internet has been closely linked to the Chinese economy, and was programmed and integrated into its macro economic development blueprints*

For instance, as early as in 1993, China established the Joint Conference on National Economic Informationization, which shouldered the responsibility of taking a leading role in building the communication network on national public economic information.

In 1997, China drew up the National Informationization Program during the 9th Five-year Plan and Goals in 2010, which brought the Internet into the construction program of national information infrastructure and proposed to boost the process of national economic informationization by striving to develop the Internet industry.

Five years later in 2002, China promulgated its Specialized Informationization Planning Program during the 10th Five-year Plan on National Economic and Social Development, which set out the priorities for China's informationization development as practicing e-government, re-energizing software industry, strengthening the development and utilization of information resources, and accelerating the development of e-commerce, etc.

In December 2002, the 16th National Congress of the CPC proposed to drive industrialization through informationization and promote informationization through industrialization, thus opening a new way of industrialization.

In November 2005, China laid down its National Informationization Development Strategy 2006-2020, which was a long-term or strategic document on informationization development, further clarified the priorities for China's Internet development, and proposed to advance national

economic informationization centered on readjusting economic structure and transforming the economic growth model. The document also proposed to practicing e-government with improving governance capacity at its core, and to carry forward social informization centering on building a harmonious society, etc.

In March 2006, the National People's Congress (NPC) examined (deliberated) and approved the 11th Five-year Plan Outline on National Economic and Social Development, proposing to boost the merger of telecommunication network, broadcast network and Internet, and to build next-generation Internet and accelerate its commercial application.

In April 2007, a meeting of the CPC Political Bureau proposed to vigorously develop cyber culture industry and cyber culture information equipment manufacturing industry. In October 2007, the 17th National Congress of the CPC established the development strategy of "developing modern industry systems, strive to integrate Informationizationand industrialization, and promote the industries to transform from being big to being strong".

In January 2010, the State Council decided to speed up the merger of the telecommunication network, broadcast network and Internet and to advance the development of information and cultural industries.

Under the Chinese government's active promotion and explicit policy guidance, China's Internet has been gradually on a road of comprehensive, sustainable and rapid development.

1.3.2. *In addition to lending full policy support to Internet development, China also invests heavily in building Internet infrastructures*

From 1997 to 2009, China invested 4,300 billion RMB in Internet infrastructure construction nationwide, and completed communication optical fiber cable covering the whole country with a total length of 8.267 million kilometers, among which 840,000 kilometers are long-distance optical cable line. By the end of 2009, China's basic telecommunication companies possessed 136 million Internet broadband access (BBA) ports, with Internet international outlet bandwidth reaching 866,367 Mbps (million bits per second), having 7 log-in submarine cables and 20 land cables with a total volume of 1,600 Gb (Gigabyte).

99.3% of China's villages and towns, and 91.5% of its administrative villages enjoy access to Internet, while 96.0% of villages and towns have access to bandwidth network.

In January 2009, the Chinese government began to provide the 3G mobile communication licenses. Now, the 3G networks have fundamentally covered the whole country. The mobile Internet is experiencing rapid development, while the Internet will benefit more people.

1.3.3. *The Chinese government actively promotes the R&D of next-generation Internet (NGI)*

During the late 1990s, China began its work on the NGI R&D and implemented a series of major science and technology programs such as "new-generation highly reliable network". In 2001, the first Chinese NGI regional experimental network, near-field communication network (NFCNET), was established in Beijing. In 2003, China Next Generation Internet (CNGI) was officially launched and marked China's entrance into a new stage of large-scale NGI

R&D and construction. Now, China has established the world's largest IPv6 excellence network, while the medium- and small-capacity IPv6 router technology, authentication technology on authentic IPv6 source address and NGI transitory technology used in the experimental network are taking a lead internationally. The technological programs proposed by China on the internationalization of domain names, IPv6 source address authentication, IPv4-IPv6 transitory technology have gained the approval of the Internet Engineering Task Force (IETF) and become part of the international Internet standards and protocols.

1.3.4. *China practices a policy of managing cyber affairs in line with law, adhering to the principles of scientific and effective administration in its Internet governance*

It also endeavors to improve its Internet governance system, which is a combination of laws and norms, administrative supervision, industry self-discipline, public monitoring and social education. Since 1994, China has promulgated a series of laws and regulations related to Internet administration. To be sure, China will continuously improve its Internet governance through practices. China also advocates the free and secure flow of Internet information, which are not only the two sides of the same coin, but also constitute an indispensable and interdependent whole. It sticks to combat cybercrimes in accordance with the laws, and opposes any form of cyber hacker behaviors, which is in line with the spirit of the Chinese laws and regulations.

1.4. Cyber legislation and Internet administration

There is much misunderstanding about China's policies and practices on Internet governance and administration. In particular, after former U.S. Secretary of State Hillary

Clinton put forward the idea of cyber freedom in her Newseum speech in January 2010, there have been increasing accusations and criticisms against China in the media and news reports, though these allegations are inconsistent with the facts and sometimes prejudiced.

In fact, China adheres to the principle of scientific and effective Internet administration by law. After years of experience, China has formulated a system of Internet governance with different layers and types of laws and regulations in place. Of course, these laws and regulations conform to the specific national conditions in China. Different from some countries' one-sided emphasis on cyber freedom, China advocates the free and secure flow of information in cyberspace, which is just like the two wings of a bird.

Along with the rapid development and changes of ICTs, China also tries to keep with the times in its cyber legislation and Internet administration. On the one hand, it sometimes revises the established laws and regulations to make them fit the new ICT environment. On the other hand, the legislative body of China also makes new laws and regulations to tackle the new problems and new phenomena brought about by the Internet and ever-changing ICTs, in particular, to deal with those negative impacts upon the political, economic, social and cultural life of the Chinese people.

1.4.1. *Basic principles and practices of Internet administration in China*

According to the *White Book on the Internet in China*, the basic goals of China's Internet administration are: to promote general and hassle-free Internet accessibility, and sustainable and healthy development, guarantee citizens' freedom of speech online, regulate the order of Internet

information transmission, promote the positive and effective application of the Internet, create a market environment for fair competition, safeguard the citizens' rights and interests vested in the Constitution and law, and ensure safety for Internet information and state security.

In practice, China adheres to the principle of scientific and effective Internet administration by law. In general, China has formulated an effective and overall system of Internet administration, which is a combination of laws and regulations, administrative supervision, self-regulation, technical protection, public supervision and social education. In addition, China also strives to improve its Internet administration system constantly.

1.4.1.1. *Laws and regulations on Internet administration*

In line with the spirit of regulating the Internet by law, China has enacted a series of laws and regulations concerning Internet administration since 1994. They include:

– Decision of the National People's Congress Standing Committee on Strengthening the Protection of Internet Information (2012);

– Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000);

– Law of the People's Republic of China on Electronic Signatures (2004);

– Regulations on Telecommunications of the People's Republic of China (2000);

– Measures on the Administration of Internet Information Services (2000);

– Regulations on the Protection of Computer Information System Security of the People's Republic of China (1994 and revised in 2011);

– Regulations on the Protection of the Right to Online Dissemination of Information (2006);

– Provisions on the Administration of Foreign-funded Telecommunications Enterprises (2001 and revised in 2008);

– Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997);

– Provisions on the Administration of Internet News Information Services (2005);

– Provisions on the Administration of Electronic Bulletin Services via the Internet (2000);

and so on……

In addition, relevant provisions of other laws are also applicable in the case of Internet administration, such as:

– Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997);

– General Principles of the Civil Law of the People's Republic of China (1986);

– Copyright Law of the People's Republic of China (1990 and its second revision in 2010);

– Law of the People's Republic of China on the Protection of Minors (1991 and revised in 2006);

– Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006);

and so on……

These laws and regulations involve basic Internet resource management, information transmission regulation, information security guarantee and other key aspects. On the whole, they define the responsibilities and obligations of basic telecommunication business operators, Internet access

service providers, Internet information service providers, government administrative organs, Internet users and other related bodies.

1.4.1.2. *The leading role of the Chinese government in Internet administration*

The Chinese government plays a leading role in Internet administration. In accordance with their statutory duties, relevant government bodies are responsible for safeguarding Chinese citizens' rights and interests, public interests and state security by law. This is also true with the cyber field. Of course, as far as the Internet is concerned, there is a division of labor among these different governmental organs.

For example, *National telecommunications administration departments* are responsible for the administration of the Internet industry, including the administration of basic resources of the Internet, such as domain names and IP addresses within China.

There is a slight administrative difference between commercial and non-commercial Internet information services in China. According to the Measures on the Administration of Internet Information Services (2000), China carries out a licensing system for commercial Internet information services and a registration system for non-commercial Internet information services respectively.

In line with the above Measures, the *publication, education, health and other* administrative *departments* implement licensing systems for "Internet information services concerning press, publication, education, medical care, medicines and medical instruments".

Public security organs and other state law-enforcement agencies bear the responsibility for Internet security supervision and administration, and investigate and punish all types of network crimes.

1.4.1.3. *Industry self-regulation*

China advocates industry self-regulation and public supervision. The practice of self-regulation by the industry is a unique feature in China's Internet governance and administration. In this regard, some professional organizations, such as the Internet Society of China (ISC), play a leading role.

Founded in May 2001, ISC is a national organization of the Internet industry with a purpose of serving the development of the Internet industry, netizens and governmental decisions. Since its foundation, the ISC has issued a series of self-disciplinary regulations, which greatly promote the healthy development of the Internet in China. These self-disciplinary regulations include:

– Public Pledge of Self-regulation and Professional Ethics for the China Internet Industry (2002);

– Provisions of Self-regulation on Not Spreading Pornographic and Other Harmful Information for Internet Websites (2004);

– Public Pledge of Self-regulation on Anti-malicious Software (2006);

– Public Pledge of Self-regulation on Blog Service (2007);

– Public Pledge of Self-regulation on Anti-Internet Virus (2009);

– Declaration of Self-regulation on Copyright Protection of China's Internet Industry (2005);

and so on……

These public pledges of self-regulation do not have legally binding power as it is up to the participants to abide by the rules, carry forward good practices while resisting and shunning away from the bad ones. Though some Western

media reports are rather caustic about this practice of self-regulation, these self-disciplinary pledges do have a kind of soft power and play a role in setting examples of good practices and shaping a clean, sound, and healthy Internet environment in China. Thus, these public pledges of self-regulation constitute a complement to the legally binding laws and regulations. For example, through the practice of self-regulatory pledges, the ISC has made unremitting efforts in helping to counter spam, reducing the global spam percentage of Chinese e-mails from 23% in 2002 to 4.1% in 2009.

1.4.1.4. *Public supervision through special websites*

With a view to strengthening public supervision of Internet services and maintaining a clean and healthy Internet environment, China has established a lot of public reporting and reception organizations since 2004. They include:

– China Internet Illegal Information Reporting Center (CIIRC)[3];

– Internet Crime Reporting Center[4];

– 12321 Harmful and Spam Internet Information Reporting and Reception Center[5];

– 12390 Pornography Crackdown and Press and Publication Copyright Joint Reporting Center[6];

and so on……

In January 2010, China also issued the Measures for Encouraging the Reporting of Pornographic and Vulgar Information on the Internet and Mobile Media. In the future,

3 http://ciirc.china.cn/.
4 http://www.cyberpolice.cn/wfjb/.
5 http://www.12321.cn/.
6 http://www.shdf.gov.cn/.

these Internet industry self-disciplinary organizations will continue to play their due role in safeguarding Internet security. The Chinese government will also further support their work in this regard and protect the public's legitimate rights to online reporting of illegal information and acts.

Moreover, China also adheres to rational and scientific law-making, and reserves space for Internet development. As the ICTs change quickly, and new cyber risks and threats are also in constant flux, the governments in the world will always be under some kind of pressure for keeping up with these changes in their cyber legislations, in order to make their laws and regulations relevant and to better protect people's interests in cyberspace. China will also revise old laws and regulations on Internet governance and enact new ones in line with the changing landscape of the ICTs and cyber risks.

1.4.2. *Guaranteeing the free and secure flow of information in cyberspace*

As mentioned above, China advocates the free and secure flow of information in cyberspace. In fact, in the Chinese philosophy, cyber freedom and cybersecurity are interwoven with and complementary to each other. Without security, the free flow of information will lose its meaning as it might be obtained and even abused by anyone else. In a similar vein, without the free flow of information, the secure flow of information will also lose its value, because, to keep the information flow secure, it will be subject to certain security measures that might undermine its availability to a wide audience. Though there is neither absolute cyber freedom nor absolute cybersecurity in cyberspace, an appropriate balance between the two have to be vigorously sought. This is what China tries to do in its cyber policies, in particular, in its cyber legislations.

1.4.2.1. *Guaranteeing Citizens' Freedom of Speech on the Internet*

The White Book on the Internet in China states that the Internet has experienced full-scope application in the news communication field of China. The Chinese government encourages and supports the development of Internet news communication undertakings, provides the public with a full range of news, and at the same time guarantees the citizens' freedom of speech on the Internet as well as the public's right to know, to participate, to be heard and to oversee in accordance with the law.

1.4.2.1.1. Constitutional guarantee

Accordingly, Chinese citizens fully enjoy freedom of speech on the Internet. The Constitution of the People's Republic of China confers on Chinese citizens the right to free speech. Therefore, with their right to freedom of speech on the Internet protected by the law, they can voice their opinions in various ways on the Internet. One of the most prominent features of China's Internet development is the vigorous online exchanges of ideas.

For example, the huge quantity of BBS posts and blog articles is far beyond that of any other country in the world. In recent years, such newly-emerging online services as blog, micro-blog, video-sharing and social networking websites are developing rapidly in China and provide greater convenience for Chinese citizens to communicate online. Now, new Internet applications and new online services, including online finance, big data and cloud computing, have provided a broader scope for people to express their opinions.

1.4.2.1.2. Public supervision via the Internet

The Chinese government has also actively created conditions for the people to supervise the government, and attaches great importance to the Internet's role in

supervision. To put it simply, the Internet's role in supervision has been brought into full play in China.

In order to facilitate the public's reporting of corrupt and degenerate officials and suchlike, the central discipline inspection and supervision authorities, the Supreme People's Court (SPC), the Supreme People's Procuratorate (SPP) and other relevant bodies have set up informant websites. The informant website of the Central Commission for Disciplinary Inspection (CCDI) of the Communist Party of China (CPC) and the Ministry of Supervision, and the website of the National Bureau of Corruption Prevention are playing an important role in preventing and punishing corruption and degeneration among officials.

1.4.2.1.3. CCDI website for public supervision

Now, the Chinese government is actively using the practice of online reporting to fight against corruption, which has greatly facilitated the government's efforts in cracking down corrupt practices and officials. For example, CCDI established and opened a website[7] in September 2013 designed to publish information, elaborate policies, solicit public opinion, and promote anti-corruption efforts through online reporting. It has a special website[8] for online reporting of corrupt practices and officials. The CCDI website also has an interactive column, which contains online interviews and a message board. In particular, the interactive column will pose one question per month to solicit visitors' opinions on certain issues. So far, for example, they include:

– How to use the Internet to carry out anti-corruption efforts (September 2013);

7 http://www.ccdi.gov.cn/.
8 http://www.12388.gov.cn/.

– How to fight against "tigers" (high-ranking officials) and "flies" (low-ranking officials) (October 2013);

– How to deal with the relationship between abiding by the law on the one hand and treasuring personal relations or feelings (worldly wisdom), in the context of fighting against the four undesirable work styles (formalism, bureaucratism, hedonism, and extravagance) (November 2013);

– What is your opinion on utilizing critical time nodes and "trifles" to firmly redress the four undesirable work styles (December 2013);

– What is your advice on making the CCDI website perform better in the new year (January 2014);

– How to achieve the goal of fighting against corruption with "zero-tolerance" (February 2014);

– What else should be done to redress the four undesirable work styles, and how (March 2014);

– Please expose the stealthy or covert forms of the four undesirable work styles (April 2014).

These questions have always been followed by numerous messages left by the visitors to the website, which greatly facilitate the anti-corruption efforts of the Chinese governments.

In addition, other Chinese governmental departments have also set up their own website for online reporting. For instance, the Central Organization Department of the CPC has established a 12380 online reporting website[9], which is also a kind of online supervision over governmental officials.

9 http://www.12380.gov.cn/.

On November 21, 2013, the Supreme People's Court (SPC) of China created official accounts on Sina Weibo and WeChat, two of the country's leading social media tools, marking its efforts to promote judicial transparency. A statement from the SPC website said the new media accounts signal the SPC's steps to boost openness, value public opinions and widen the channel for the masses to oversee judicial authorities, which are in line with the spirit of the Third Plenary Session of the 18th Communist Party of China (CPC) Central Committee held in November 2013. The Chinese Netizens hailed it as "a milestone for China's rule of law" in the comments posted on the court's micro-blog account.

The above efforts and practices reflect not only the increasing openness and transparency of the Chinese government in its daily work, but also its willingness to solicit good opinions and advice from the people, much larger in number than that of governmental officials, to improve its daily work and even work styles. Now, the opinions expressed by the public online are receiving unprecedented attention. In other words, the Internet has become a new channel for the Chinese government to get to know the people's situation and amass the public's wisdom, and consequently exercise governance for the people and improve its work.

To quote the *White Book on the Internet in China*, the Internet provides unprecedented convenience and a direct channel for the people to exercise their right to know, to participate, to be heard and to oversee, and is playing an increasingly important role in helping the government get to know the people's wishes, meet their needs and safeguard their interests. In a word, the Chinese government is determined to unswervingly safeguard the freedom of speech on the Internet enjoyed by Chinese citizens in accordance with the law.

1.4.2.1.4. Protecting citizens' online privacy

As more cases of Internet users' information being leaked are emerging, the protection of citizens' online privacy is becoming high on the Chinese government's agenda, because it is closely connected with the people's sense of security and confidence in the Internet. In fact, there are already provisions in the existing Chinese laws and relevant regulations.

For instance, the Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000) stipulates that illegal interception, tampering with or deletion of others' e-mails or other data and infringement upon citizens' freedom and privacy of correspondence that constitutes a crime shall be investigated for criminal liability in line with the Criminal Law.

Moreover, according to the self-disciplinary public pledges of the Internet industry (2002), Internet service providers are responsible for protecting users' privacy. The providers shall publish their relevant privacy protection commitment when providing services, provide reporting and reception channels for privacy infringement and take effective measures to protect users' privacy.

Of course, the Chinese government will always improve relevant legislation and Internet corporate service regulations, in order to steadily enhance online privacy protection systems.

1.4.2.1.5. Guaranteeing online safety for minors

Minors have become China's biggest online group. Therefore, the Chinese government attaches great importance to online safety for minors, and has always prioritized the protection of minors in the overall work of Internet information security programs.

The Law of the People's Republic of China on the Protection of Minors (1991 and revised in 2006) stipulates that the state shall take measures to prevent minors from overindulging in the Internet and to prohibit any organization or individual from producing, selling, renting or providing by other means electronic publications and Internet information containing pornography, violence, murder, terror, gambling or other contents harmful to minors.

In recent years, more and more people and organizations in China are calling for special laws and regulations concerning guaranteeing the online safety for minors. In particular, China advocates that families, schools and all other social units shall work together to protect minors online and create a healthy online environment for the development of minors.

From late September to November 2013, the State Internet Information Office (SIIO), the Ministry of Education (MOE), the Central Committee of the Communist Youth League of China and the All-China Women's Federation (ACWF) jointly initiated a two-month campaign dubbed "Green Web" to tighten supervision of websites and cell phone applications to fight lewd content and aggressive remarks aimed at young people. A statement released by the SIIO said that the move aims to further cleanse the Internet environment, provide a healthy and positive online environment for young people and protect their legal interests.

1.4.2.2. *Protecting Internet Security*

The White Book on the Internet in China says that Internet security is a prerequisite for the sound development and effective utilization of the Internet. The Chinese government holds that the Internet is an important national infrastructure. Therefore, within Chinese territory, the

Internet is under the jurisdiction of Chinese sovereignty, and the Internet sovereignty of China should be respected and protected. Accordingly, citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and protect Internet security.

First, China protects Internet security in accordance with the law. Numerous related rules are included in the existing Chinese laws and regulations in order to promote the sound development of China's Internet, protect state security, social and public interests, and lawful rights and interests of individuals, legal persons and other organizations. These laws and regulations include:

– Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997);

– Decision of the National People's Congress Standing Committee on Strengthening the Protection of Internet Information (2012);

– Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000);

– Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006);

– Regulations on Telecommunications of the People's Republic of China (2000);

– Regulations on the Protection of Computer Information System Security of the People's Republic of China (1994 and revised in 2011);

– Measures on the Administration of Internet Information Services (2000);

– Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997);

and so on……

For instance, Article 6 of the Regulations on Telecommunications of the People's Republic of China (2000) stipulates that "the security of telecommunications networks and information shall be protected by law. No organization or individual may utilize telecommunication networks to engage in activities that jeopardize state security, the public interest or the legitimate rights and interests of other people".

Second, China protects the secure flow of information. China believes that the free and secure flow of Internet information is an integral whole. To put it differently, on the premise of protecting the safe flow of Internet information, the free flow of Internet information may be realized. Therefore, the Chinese government attaches great importance to protecting the secure flow of Internet information, actively guides people to manage websites in accordance with the law and use the Internet in a wholesome and correct way.

The Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000), Regulations on Telecommunications of the People's Republic of China (2000), and Measures on the Administration of Internet Information Services (2000) contain clear stipulations that no organization or individual may produce, duplicate, announce or disseminate information having the following contents:

– being against the cardinal principles set forth in the Constitution;

– endangering state security, divulging state secrets, subverting state power and jeopardizing national unification;

– damaging state honor and interests;

– instigating ethnic hatred or discrimination and jeopardizing ethnic unity;

– jeopardizing state religious policy, propagating heretical or superstitious ideas;

– spreading rumors, disrupting social order and stability;

– disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime;

– humiliating or slandering others, trespassing on the lawful rights and interests of others;

– other contents forbidden by laws and administrative regulations.

It is noteworthy that these regulations are the legal basis for the protection of Internet information security within the territory of the People's Republic of China. In addition, all Chinese citizens, foreign citizens, legal persons and other organizations within the territory of China must obey these provisions.

Third, China opposes all forms of computer hacking. China is one of the countries suffering most from hacking. Like other countries, China faces a severe challenge of online criminal activities such as computer hacking and viruses. Chinese laws prohibit all forms of hacking compromising Internet security.

For example, the Decision of the National People's Congress Standing Committee on Guarding Internet Security (2000) stipulates that acts deconstructing Internet security which constitute crimes, such as "intentionally inventing and spreading destructive programs such as computer viruses to attack the computer system and the communications network, thus damaging the computer system and the communications network", shall be

investigated for criminal liability in accordance with the relevant provisions in the Criminal Law.

Likewise, Articles 285 and 286 of the Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997) contain concrete provisions on the criminal punishment of illegal activities such as illegally obtaining data stored in or handled or transmitted by the computer information system, or providing destructive programs or tools for invasion and illegal control of computer information systems.

Fourth, China combats computer crime in accordance with the law. In recent years, computer crimes in China have been on the increase. Online fraud, online theft and other forms of crimes encroaching on the property of others are increasing rapidly. In order to effectively combat computer crimes, the Chinese laws stipulate that criminal activities conducted by making use of the Internet or against the Internet shall be investigated and dealt with in accordance with the Criminal Law of the People's Republic of China (1979 and its fifth revision in 1997); if such activities are not serious enough to constitute crimes, administrative punishment shall be meted out in accordance with the Law of the People's Republic of China on Punishments in Public Order and Security Administration (2006) and Measures on the Administration of Security Protection of the International Networking of Computer Information Networks (1997).

On the operational level, the Ministry of Public Security (MPS) has established a Bureau for Cybersecurity Protection, which is especially devoted to combating cybercrimes. It also conducts international cooperation in this regards. For instance, China and the United States have carried out cooperation in fighting against cybercrimes.

In brief, cyber freedom and cybersecurity are the two sides of the same coin. In general, the Chinese government has actively explored channels and methods of scientific and effective Internet administration by law, and has formed a preliminary Internet administration model that is suitable for China's conditions and consistent with international practices. Of course, Internet administration is a process of continuous practice, and the Chinese government will further improve its efforts on Internet administration.

1.5. Cybersecurity and diplomacy: an international perspective

In an interconnected cyber world, there is neither absolute security nor absolute freedom for anyone or any state. In other words, any country could not go it alone in the interdependent cyber world. In another sense, though connected, the Internet of various countries belongs to different sovereignties, which also makes it necessary to strengthen international exchanges and cooperation in this field. Therefore, cyber cooperation is of both practical and strategic necessity. In the future, all countries should enhance international and bilateral cyber exchanges and cooperation, learn more about each other's concerns, and build mutual trust in order to build a peaceful, secure and open cyberspace.

According to the *White Book on the Internet in China*, China maintains that all countries should, on the basis of equality and mutual benefit, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security, promote the healthy and orderly development of the industry, and share the opportunities and achievements brought about by this development.

In practice, China has promoted international cooperation on cyber issues in an active manner. By now, it has conducted various strategic and security dialogues and consultations on cybersecurity with numerous countries, carried out legal cooperation on fighting against cybercrimes, engaged in technical cooperation in addressing cyber incidents on a daily basis, and so on. All these are signs of China being sincere, open and practical to international cybersecurity dialogue and cooperation. To put it simply, international cooperation on cybersecurity has become an inherent part of China's policies, practices and even strategy.

1.5.1. *Cyber policy dialogue and consultation*

China actively promotes the establishment of bilateral dialogue and exchange mechanisms in the field of the Internet, through which China and relevant countries exchange their policies and practices on the Internet development and cybersecurity, know more about and learn from each other, increase mutual understanding, build confidence and mutual trust, thus contributing the Internet development and cybersecurity.

For example, in their Strategic Security Dialogue under the framework of China-U.S. Strategic and Economic Dialogue (S&ED), China and the United States have touched upon and begun to talk about cybersecurity issues. During U.S. Secretary of State John Kerry's visit to Beijing in April 2013, the two sides decided to set up a working group on cybersecurity within the framework of the China-U.S. S&ED. In their meeting, Chinese Foreign Minister Mr Wang Yi told Kerry that China and the United States should make joint efforts to safeguard cyberspace, which should be an area where the two countries can increase mutual trust and cooperation.

The first China-U.S. cybersecurity working group meeting was held on July 8, 2013 in Washington, ahead of the 5th round of the China-U.S. S&ED taking place on July 10-11, 2013. Under the context of whistleblower Edward Snowden's revealing of the bulk Internet and telephone surveillance over American and non-American citizens conducted by the U.S. National Security Agency (NSA), the cybersecurity issue undoubtedly became a hot topic during the S&ED.

The two sides held candid and in-depth exchanges on the improvement of the cyber working group mechanism, cyber ties between the two countries, international cyberspace regulations and a bilateral dialogue on and cooperation in cybersecurity. China and the U.S. reportedly hope to create the mechanism under the principals of mutual respect and equal dialogue, so that the working group can play a positive role in enhancing mutual trust, reducing differences and expanding cooperation in cybersecurity. The two sides also agreed to hold another meeting within the year.[10]

On December 3, 2013, the working group held another meeting in Beijing, during which the two sides held a candid, in-depth and constructive dialogue and reached good results. They thought positively of the relevant exchanges and cooperation in the cyber field between the two sides since their first meeting in July 2013. They also expressed their willingness to strengthen the dialogue and cooperation, and to manage and control their disputes, with a view to promoting the sound interaction in the cyber field between the two sides, on the basis of mutual respect and win-win

10 Zhang Ming'ai, "Cybersecurity tops China-US S&ED agenda", July 10, 2013, http://www.china.org.cn/world/2013-07/10/content_29382578.htm

cooperation. Officials and experts from numerous departments of the two countries attended the meeting.[11]

China has also held cybersecurity dialogues and consultations with France, Germany, South Korea, the European Union, and other countries and organizations in recent years. Moreover, as of the end of 2013, the State Council Information Office and the State Internet Information Office of the People's Republic of China have hosted China-U.S. Internet Industry Forum (6 times) and China-UK Internet Roundtable (5 times), China-South Korea Internet Roundtable (2 times) with the United States, the United Kingdom and the Republic of Korea respectively since 2007.

To draw on the experience of other countries in developing and administering the Internet industry, the Chinese government has organized dozens of delegations since 2000 to visit dozens of countries in Asia, Europe, North America, South America and Africa, and has learnt and applied some of their successful experiences to its own Internet development and administration.

1.5.2. *Regional cyber cooperation*

China attaches great importance to regional cooperation in maintaining Internet security. As early as in 2009, China signed the China-ASEAN Coordination Framework for Network and Information Security Emergency Responses,

11 On the Chinese side, they include the Ministry of Foreign Affairs, the Ministry of National Defense, the Ministry of Public Security, the Ministry of Industry and Information Technology, the State Council Information Office. On the American side, they include the Department of State, the National Security Council of the White House, the Department of Defense, the Department of Homeland Security, Department of the Treasury, and FBI. See "China-U.S. Working Group on Cybersecurity holds a meeting in Beijing", December 4, 2013, http://www.fmprc.gov.cn/mfa_chn/wjb_602314/zzjg_602420/bmdyzs_602866/xwlb_602868/t1105394.shtml.

and the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, with the ASEAN and SCO member states respectively.

In September 2013, China hosted an "ASEAN Regional Forum (ARF) Workshop on Measures to Enhance Cybersecurity – Legal and Cultural Aspects" in Beijing, trying to build regional consensus and work out practical measures on cybersecurity. China also participate in the work and activities on cybersecurity within the framework of the Council for Security Cooperation in the Asia-Pacific (CSCAP), Asia-Pacific Economic Cooperation (APEC), and the Conference on Interaction and Confidence-Building Measures in Asia (CICA), etc.

On April 2, 2014, China issued a policy paper on the European Union (EU)[12], which contains both the macro goals and the micro measures on promoting China-EU cooperation on cybersecurity. On the macro level, it states that China and the EU should "strengthen cybersecurity dialogue and cooperation and promote the building of a peaceful, secure, open and cooperative cyberspace", and "facilitate practical cooperation between China and the EU in fighting cyber-crimes, emergency response to cybersecurity incidents and cyber capacity building through platforms such as the China-EU Cyber Taskforce and work together for the formulation of a code of conduct in cyberspace within the UN framework".

On the operational level, it says that the two sides should "strengthen China-EU Dialogue on Information Technology, Telecommunication and Information, conduct exchanges and dialogue on related strategies, policies and regulations and

12 "China's Policy Paper on the EU: Deepen the China-EU Comprehensive Strategic Partnership for Mutual Benefit and Win-win Cooperation", April 2014, http://news.xinhuanet.com/english/china/2014-04/02/c_133230788_2.htm.

actively promote cooperation and exchanges on trade in IT products and industrial technology", "encourage broader exchanges on intellectual property rights and technical standards and continue to raise the level of China-EU cooperation on intellectual property rights", and "strengthen China-EU cooperation and exchanges on information security, especially cybersecurity".

1.5.3. *Track Ⅱ cyber diplomacy*

In addition to official exchanges and cooperation with other countries, China also carries out Track Ⅱ cyber activities. For instance, the Internet Society of China (ISC) and the U.S. think tank EastWest Institute (EWI) conducted a joint research and released a report on "Fighting Spam to Build Trust" in June 2011[13]. Two years later, the ISC and EWI presented another joint report *Frank Communication & Sensible Cooperation to Stem Harmful Hacking* at the EWI-IEEE World Cyberspace Cooperation Summit held at Stanford University in November 2013.[14]

Moreover, the China Institute of Contemporary International Relations (CICIR) and the Center for Strategic and International Studies (CSIS) of the United States have held seven formal meetings on cybersecurity (accompanied by several informal discussions) since 2009, called "Track Ⅱ China-U.S. cybersecurity Dialogue". According to the CSIS website introduction, the goals of the discussions have been to reduce misperceptions and to increase transparency of both countries' authorities and understanding on how each country approaches cybersecurity, and to identify areas of

13 "Fighting Spam to Build Trust", EastWest Institute and Internet Society of China, June 2011.

14 Karl Frederick Rauscher and Zhou Yonglin, *Frank Communication & Sensible Cooperation to Stem Harmful Hacking*, November 2013, http://www.isc.org.cn/download/China-U.S.%20Anti-Hacking%20Report.pdf.

potential cooperation, including confidence building measures and agreement on norms and rules for cybersecurity. The meetings have been attended by a broad range of Chinese and U.S. officials and scholars responsible for cybersecurity issues.[15]

1.5.4. *Legal cooperation in combating cybercrimes*

As cybercrimes have become increasingly rampant in recent years, and given the fact that cybercrime constitutes the bulk of malicious cyber activities, China has participated actively in international cooperation on combating cybercrime. According to the *White Book on the Internet in China*, in combating network crimes, the Chinese public security organ has participated in the Interpol Asia-South Pacific Working Party on IT Crime, China-US Joint Liaison Group (on Law Enforcement) and other forms of international cooperation, and has conducted bilateral and multilateral meetings successively with such countries or regions as the US, the UK, Germany, Italy and Hong Kong.

The Council of Europe Convention on Cybercrime or Budapest Convention on Cybercrime is a vanguard in combating cybercrimes.[16] The Convention plays a constructive role in promoting international judicial cooperation on fighting against cybercrimes. However, the Convention, which was formed in 2001, also has its inherent deficiencies, such as an inadequate voice and representation for the developing countries and therefore fails to adequately reflect the concerns of the developing world in fighting cybercrime. In particular, there is regulation about extraterritorial jurisdiction, which might constitute a

15 See CSIS website http://csis.org/program/china-institute-contemporary-international-relations-cicir.

16 See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

violation of state sovereignty and be incompatible with domestic legislations in case of a transnational collection of evidence. As a result, China has not signed it until now. However, it has participated in relevant activities concerning the Convention, expressed its views on relevant matters, and conducted wide-ranging practical communications with other countries and organizations on this. In other words, accession to it or not has not been a precondition for carrying out practical exchanges and cooperation on the ground. In essence, with or without it, there would be successful international cooperation on dealing with cybercrimes.

For example, China's Policy Paper on the EU discussed above states that China will "advance China-EU cooperation on police law enforcement, implement the five-year police training cooperation project, expand exchanges on policing administration, public security management, law enforcement regulation, criminal investigation technologies and the fight against organized crimes by organizing training courses, visits and seminars, increase the mutual trust between the two sides, and lay a solid foundation for jointly combating terrorism, economic, cyber and drug-related crimes, organized illegal immigration and other serious organized transnational crimes". This fully demonstrates the willingness and sincerity of China to engage in practical cooperation with other countries and organizations on fighting against cybercrimes.

In practice, the Chinese public security bodies handled from 2006 to 2009 more than 500 letters of assistance in case handling from more than 40 countries and regions concerning network crimes, which cover many types of cases, including hacker attacks, child pornography and network fraud.

1.5.5. *Technical cooperation*

On a technical level, it is easier for countries to cooperate with each other. The Ministry of Industry and Information Technology (MIIT) is the main governmental department responsible for IT research and development, relevant policies, and international technological cooperation, though other departments might also cover certain aspects of technical matters. Some major Internet security companies, such as China Mobile, China Unicom, China Telecom, and others also have an important role to play in China's Internet development and cybersecurity.

In addition, some professional organizations are inalienable for China's Internet security and international cyber cooperation, including the Internet Society of China (ISC), the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT/CC), and the China Internet Network Information Center (CNNIC), and so on.

1.5.5.1. *CNCERT*

The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT or CNCERT/CC) is an organization of network security technical coordination. Since its foundation in September 1999, CNCERT has been dedicated to carrying out the work of preventing, detecting, warning and handling China network security incidents under the policy of "positive prevention, timely detection, prompt response, guaranteed recovery", to maintain the safety of China's public Internet and ensure the safe operation of the information network infrastructures and the vital information systems.

Branches of CNCERT have spread in all provinces, autonomous regions and municipalities in mainland China. As China's core technical coordination organization,

CNCERT is playing a vital role in coordinating all Computer Emergency Response Teams within the country to handle cybersecurity incidents jointly.

CNCERT is active in developing international cooperation and is a window for handling network security incidents with the world. As a full member of the famous international network security cooperative organization FIRST and one of the initiators of APCERT, CNCERT devotes itself to building a prompt response and coordination handling mechanism of cross-border network security incidents. By 2013, CNCERT had established "CNCERT International Partners" relationships with 127 organizations from 59 countries or regions.[17] Therefore, CNCERT engages in practical and technical cooperation with other countries in addressing cross-border cybersecurity incidents.

In addition to the International Partnership program, it has also officially signed memorandums of understanding (MOUs) on cybersecurity cooperation or reached agreements with dozens of the above-mentioned organizations, and has gradually improved and enhanced the collaborative mechanisms on addressing cross-border cybersecurity incidents.

For instance, in 2012, it tackled 4,063 cybersecurity incidents involving elements within China (an increase of 3 times as many as that of 2011) in coordination with overseas security organizations, and assisted foreign agencies in addressing 961 cybersecurity incidents, an increase of 69.2% compared with that of 2011. These cybersecurity incidents included not only those DDoS attacks and phishing activities against China, but also those against foreign banks and companies, such as the Bank of America (BOA), the National Australia Bank, and PayPal. In October 2012, CNCERT received a complaint from the USCERT, which claimed that

17 http://www.cert.org.cn/publish/english/index.html.

some of the host computers located in China were controlled by malwares and participated in DDoS attacks against certain US banks and companies, and asked China for assistance in dealing with them. After some examinations, CNCERT addressed 75 IP addresses, provided by the USCERT, in a timely manner. Moreover, CNCERT also cracked down on a botnet named Nitol together with the Microsoft Corporation, in which the domain name 3322.org, used to spread and control malwares, was eliminated and more than 70,000 malicious domain names were closed.[18]

CNCERT also publishes weekly, monthly and annual reports on cyber threats and the cybersecurity situation in China, from which we can see that every week it deals with dozens or even hundreds of transnational cyber incidents together with its counterparts from other countries. It also participates in APCERTS' annual exercises, provide relevant training courses and programs to ASEAN members, engage in bilateral and multilateral cooperation with other countries and regional and international organizations, thus greatly facilitating and contributing to the Internet security all over the world.

1.5.5.2. *CNNIC*

The China Internet Network Information Center (CNNIC) is an administration and service organization that was set up on June 3, 1997 upon the approval of the competent authority which undertakes the responsibilities as the national Internet network information center.

---

18 National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cybersecurity Posture in 2012*, 19 March 2013; 国家互联网应急中心：《2012年我国互联网网络安全态势综述》，2013年3月 http://www.cert.org.cn/publish/main/46/2013/20130320093925791767941/20130320093925791767941_.html.

Its overall task is to "provide efficient and application-oriented services through secure and stable Internet infrastructure for public interests". As an important constructor, operator and administrator of infrastructure in Chinese information society, CNNIC is responsible for the operation, administration and services of fundamental Internet resources. It also undertakes R&D and security work of fundamental Internet resources, conducts research on Internet development and provides consultancy, and promotes the cooperation and technological exchange of global Internet in an effort to become an excellent network information center.

Its main responsibilities[19] include: (1) operation, administration and service organization of national network fundamental resources[20]; (2) research, development and security center of national network fundamental resources[21]; (3) research and consulting service driving force for Internet

19 See http://www1.cnnic.cn/AU/Introduction/Introduction/201208/t20120815_33295.htm.

20 CNNIC is a registry of domain names and root zone operator. It operates and administers country code top level domain of .CN and Chinese domain name system, and provides 24-hour services of domain name registration and resolution as well as WHOIS lookup for worldwide users with its professional technologies. CNNIC is a member of Asia-Pacific Network Information Center (APNIC) as a National Internet Registry (NIR). As the convener of IP Address Allocation Alliance, CNNIC is responsible for providing allocation and administration services to China's Internet service providers (ISPs) and Internet users and promoting the transition to Internet of next-generation based on IPv6 in China.

21 CNNIC constructs a world-leading, efficient and safe & stable service platform for fundamental network resources. It provides multi-level and multi-mode not-for-profit services for fundamental network resources, and seeks to make a breakthrough in the core competence of fundamental network resources and self-developed devices and softwares so as to improve the reliability, security and stability of China's system of fundamental network resources.

development[22]; (4) platform for Internet open cooperation and technical exchange.

In particular, CNNIC tracks the latest development of Internet policies and technologies and has business coordination and cooperation with relevant international organizations and the Internet network information centers in other countries and regions. In addition, CNNIC hosts important international conferences and activities concerning the Internet, and creates an open research environment and platform for international exchange and sharing. In this way, it promotes the application of scientific research achievements and development of China's Internet.

1.5.5.3. *ISC*

The Internet Society of China (ISC) was inaugurated on May 25, 2001. It is sponsored by more than 70 sponsors, including network access carriers, ISPs, facility manufacturers and research institutes, etc. It has more than 400 members covering legal companies, research institutes, academic associations, universities and other organizations engaged in various activities related to the Internet. The main mission of ISC is to promote development of the Internet in China and make efforts to construct an advanced information society. ISC is also expected to be a link among the community to make efforts benefiting the whole industry, to push forward industry self-discipline, to strengthen communication and cooperation between its

22 CNNIC is responsible for conducting surveys about the Internet including surveys on the development status of China's Internet, and it gives a description of the macroscopic picture of the development status of China's Internet and records its development faithfully. CNNIC will continue to beef up its support for the research of government policies on the one hand and provide not-for-profit research and consulting services for Internet development for enterprises, users and research institutes on the other hand.

members, to assist and provide support for making policies, and to promote Internet application and public awareness.[23]

1.5.6. *Office for Cyber Affairs of the MFA*

To deal with increasingly prominent cybersecurity issues and enhance intra-governmental coordination on the external aspects of cyber affairs, the Ministry of Foreign Affairs established the Office for Cyber Affairs in June 2013, whose responsibility is to coordinate and conduct diplomatic activities related to cyber affairs.[24] Then, Mr. Fu Cong, a counselor from the Department of Arms Control of MFA was appointed as the Coordinator for Cyber Affairs. Mr. Fu has rich diplomatic experiences. He once served as an adviser to the Director-General of the World Health Organization (WHO).[25]

Though the MFA does not enjoy an advantage over technological details, it has rich experiences in dealing with international affairs. As the Internet has a transnational feature, as ICTs can be commanded by anyone with some

23 About Internet Society of China, see http://www.isc.org.cn/english/About_Us/Introduction/.

24 http://www.fmprc.gov.cn/mfa_chn/wjdt_611265/fyrbt_611275/t1050377.shtml.

25 Fu Cong, a Chinese national, is adviser to the Director-General. His diplomatic career began when he joined the Chinese Foreign Ministry in 1987. He has served in posts based in Beijing and overseas in Geneva and Vienna. He became Deputy Director General of the Arms Control Department of the Chinese Foreign Ministry in 2003, and was the Deputy Director General of the Foreign Affairs Office of China's Xinjiang Autonomous Region from 2004-2005. From September 2005 to October 2007, Mr. Fu worked as a minister-counselor in China's Permanent Mission in Geneva. He worked on many issues, including those related to the international organizations based in Geneva, including WHO, the World Intellectual Property Organization and the International Telecommunication Union. Mr. Fu graduated from the Foreign Affairs College in Beijing, China and studied at the Polytechnic of Central London in the United Kingdom. He is married with one child. See http://www.who.int/dg/office/cong/en/index.html.

computer expertise or skills, as cyber threats and cybercrimes do not respect sovereign borders, every Foreign Ministry in the world could play an important role in coping with the international aspects of cyber issues, in addressing trans-border cyber risks, threats, and incidents, in fighting against cybercrimes, in engaging in international cooperation, building mutual trust, and maintaining international order in cyberspace.

Therefore, it is expected that the Office of Cyber Affairs under the MFA of China will also play its due roles in cyber issues. One the one hand, it could present China's ideas, visions and interests to the outside world; on the other hand, as its mission states, it could coordinate and conduct diplomatic activities related to cyber affairs.

All of the above are signs of China being open and cooperative in the cyber field and constitute a starting point for future international cooperation with a view to building a peaceful and secure cyberspace for all.

1.6. A cybersecurity strategy in the making?

In recent years, the number of cyber-attacks has increased significantly, the occurrence of cyber incidents has become more frequent, and cyber-attacks *per se* have become increasingly complex. As a result, more and more countries have become some kind of victims of cyber-attacks on the one hand, and have realized the seriousness of cyber-attacks and the importance of cybersecurity on the other hand. Therefore, numerous countries have published their cybersecurity strategies, which usually acknowledge both the benefits and damages that the Internet has brought about to humankind and people's daily life, clarify the goals and objectives they want to achieve in cyberspace, and define the means of tackling cyber threats and safeguarding cybersecurity.

Under this context, many people have asked whether China has a cybersecurity strategy and, if not, whether China should have such a strategy and when China will have such a strategy. With regard to the former, literally, the answer is no. So far, China has not published such a policy paper as a cybersecurity strategy. However, the Information Office of the State Council did published a *White Paper on the Internet in China* in June 2010, which is a comprehensive introduction about the development of the Internet in China, as well as China's policy and practices on cyber issues.

As for the latter, though there is not an assured answer to the "when" question, the answer to the "whether" question would be yes for several reasons. First, in recent years, China has also suffered from increasing cyber-attacks, and it needs a strategy to deal with those various cyber threats. Second, as more and more countries in the world have produced their cybersecurity strategies, China is also under a kind of international peer pressure to have one of its own making. Third, just like other countries, different governmental departments are in charge of different aspects of ICT issues, such as Internet development, information and communication technologies, and international exchanges, though there are some overlaps with regard to some of their functions. So, there is a lack of a central and coordinating body covering the full-spectrum of cybersecurity issues. To put it differently, there is a question of "calling whom" when a cyber incident occurs or submitting a report to whom when there are some reports and suggestions regarding cyber affairs.

As a matter of fact, there are many voices in China calling for the government to produce a cybersecurity strategy and establish a special administrative organization to coordinate and manage those issues connected with cybersecurity. For instance, the National Computer Network Emergency

Response Technical Team/Coordination Center of China (CNCERT/CC) puts forward such advice almost every year in its annul reports on China Cybersecurity Posture.[26] Many scholars also have similar ideas in their academic writings and reports. Now, their efforts begin to yield results.

Facing the increasingly severe cybersecurity situation, the Chinese government has sensed the need to increase the coordination between different governmental departments, different sectors, and different layers of work in the field of ICT. Now, the highest authority begins to take action. On February 27, 2014, the Central Leading Group on Internet Security and Informationization held its first meeting in Beijing.

According to a statement released after the first meeting of the group, President Xi Jinping will head the central Internet security and informatization leading group. Premier Li Keqiang and Liu Yunshan, who are both members of the Standing Committee of the Political Bureau of the Communist Party of China Central Committee, are the group's deputy heads. Members of the group also adopted the group's work rules and its working plan for this year at the meeting.

President Xi presided over the meeting, stressing that Internet security and informatization is a major strategic issue concerning a country's security and development as well as people's life and work. He said that "efforts should be made to build our country into a cyber power". Therefore, the group is designed to lead and coordinate Internet security

26 National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *China Cybersecurity Posture in 2012*, 19 March 2013; 国家互联网应急中心：《2012年我国互联网网络安全态势综述》，2013年3月。http://www.cert.org.cn/publish/main/46/2013/20130320093925791767941/20130320093925791767941_.html.《2013年我国互联网网络安全态势综述：CNCERT观点》。

and informatization work among different sectors, as well as draft national strategies, development plans and major policies in this field.

The president also noted that China has the world's largest number of Internet users but still lags behind in the development of Internet technologies. In addition, the digital gap between rural and urban areas remains large and the average bandwidth enjoyed by each Chinese person is far less than that in some developed countries. For instance, by the end of 2013, China reported about 618 million Internet users, but only 28.6 percent of them live in the countryside. President Xi emphasized that "we should be fully aware of the importance and urgency of Internet security and informatization". The president also said that China has to balance its needs of developing IT technologies and safeguarding Internet security, describing the two issues as two wings of a bird and two wheels of an engine.[27]

Now that the Central Leading Group on Cybersecurity and Informationization has been established and convened its first-ever meeting, we believe that it will play an increasingly important and substantial role in coordinating cybersecurity affairs on the highest level of authority in the future.

With the Central Leading Group now being in place, it is expected to carry out its functions and duties as set out during its first meeting. In particular, it will play a bigger role in formulating cyber policies on the strategic level or of strategic significance. Accordingly, a Chinese version of cybersecurity strategy might emerge in the future.

27 "Xi heads Internet security group", xinhuanet, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148418.htm.

To put it literally, a strategy usually contains two basic components: one is to clarify and define the goals or objectives one wants to achieve, while the other is to find out and shape the means or ways of realizing the established goals and objectives. In essence, a strategy requires a match between the goals and means. If there is a mismatch, a strategy will run into problems.

As with other countries' cybersecurity strategies, the Chinese one will also include the following contents: to demonstrate the significance and meaning of Internet development for China, define cyber goals and objectives China wants to achieve in cyberspace, identify possible cyber risks and threats China might face, and figure out feasible policy measure.

1.6.1. *Significance of the Internet for China*

As argued above, there is no doubt that the Internet is of great significance for China's reform, opening up, development and modernization cause. This will also be the case for China in the future. Just like the United States, China will be another country in the world to have a high-degree of reliance upon the Internet and ICTs.

1.6.2. *Goals and objectives*

The overall goal of China's cyber policy is to maintain and build a peaceful, secure, open and cooperative cyberspace, for the benefits of both the Chinese people and humankind as a whole.

1.6.3. *Cyber threat landscape*

Just like the rapid development of ICTs *per se*, the threats, risks and vulnerabilities inherent in or accompanying ICTs also change continuously. Therefore, the

threat landscape will change constantly, which poses the biggest challenge for China's cybersecurity.

China has made great progress in developing its Internet, but as with others, it also faces various security challenges in cyberspace. In fact, China has been a major victim of cyber-attacks, which have been increasing dramatically in recent years and fully demonstrated China's weaknesses in the realm of cybersecurity.

First, although China has made due progress in its information and communication technologies (ICTs), as a late comer to this field, it still lags far behind other developed countries in many areas.

It would take a rather long time for China to narrow its technological gap with that of the advanced countries. In particular, numerous core cyber technologies are in the hands of Western countries, who enjoy a formidable technical edge and are at the upper stream of producing computer chips and web devices, while China is at the downstream of the supply chain, putting it in a disadvantageous position. The imbalances in the development of cyber capabilities between different regions and between urban and rural areas just make the situation even worse. Accordingly, China is in a state of cyber insecurity, with the recent Snowden and Prism event being a case in point. In the near future, this would be a fundamental challenge for China to safeguard its cybersecurity.

Second, although China has the largest number of netizens in the world, many of them are just green hands in accessing ICTs, often without any awareness or sense of cybersecurity.

Even the more educated people have little knowledge about cybersecurity, let alone the vast majority of the

common people. Upgrading software or patching security flaws might be easy, but people have to be alerted and told first of all and then educated on cyber (in)security. Briefly, a lack of cybersecurity awareness poses a direct threat herein.

Third, China is also faced with international peer pressures in cybersecurity.

Over recent years, numerous countries have strengthened their cybersecurity measures, *inter alia*, by building cyber armies. In particular, the U.S. established its Cyber Command in 2009 with a view to enhancing its offensive cyber capabilities. Many other countries are also busy with building their cyber armies, developing cyber weapons, conducting cyber exercises, and making ambitious cybersecurity policies. Although these moves are said to be defensive, many are of the nature of building offensive cyber capabilities, which could pose a serious threat to other countries, China included. These days, more and more people are also talking about the cyber arms race, which is surely an ominous trend that should be curbed and resisted.

Fourth, China is suffering from various cyber-attacks in the real world as well as in cyberspace.

China's Internet security watchdog CNCERT released a report covering 2013 on March 28, 2014. The report says that cyber-attacks from overseas on China's Internet are on the rise, while backdoor threats, phishing and trojans or botnets constitute three main forms of attack. In 2013, 31,000 overseas mainframes controlled 61,000 websites on the Chinese mainland through backdoor programs. Despite an annual decrease of 4.3 percent in the number of mainframes involved, the number of affected websites was up 62.1 percent compared to the previous year. Some 15,349 websites, about a quarter of the total, were attacked by 6,215 mainframes located in the United States. Moreover, 90.2 percent of phishing websites targeting Chinese users

were running on foreign servers. A total of 3,823 overseas IPs lured Chinese users to 29,966 fake websites to obtain passwords and other personal information, up 54.3 percent and 27.8 percent year on year respectively. U.S.-based servers hosted 12,573 fake phishing websites. In addition, 29,000 overseas servers controlled 10.9 million mainframes on the Chinese mainland via trojans or botnet. Servers originating from the United States hijacked 41.1 percent of all the mainframes, followed by those from Portugal and the Republic of Korea. The report suggests China map out a state-level strategy and devise more regulations to enhance cybersecurity.

Moreover , according to the reports by *Der Spiegel* and the *New York Times* based on the materials leaked by former NSA (National Security Agency of the United States) contractor Edward Snowden, the NSA conducted surveillance against the Chinese Huawei company, former Chinese top leaders, thus posing a severe threat to China's cybersecurity. So, in technical and real terms, China is faced with a severe cybersecurity situation.

1.6.4. *Means for strategic goals*

As for the policy measures, several aspects deserve our attention here.

First, China should have a deeper understanding and conduct more research on cybersecurity, including its technical, policy, strategic, economic, political, social, military, legal and international aspects. In particular, China should raise its awareness on cyber threats and cybersecurity.

Second, China should build its technical capabilities and narrow digital gaps. Just as mentioned above, disadvantages in cyber capabilities constitute a fundamental challenge to

China's cybersecurity. Therefore, in the future, China still needs to upgrade its cyber capabilities, including improving its cyber infrastructure, thus gradually narrowing its digital gaps with the more advanced countries.

Moreover, China will also provide due help and aid to other developing countries in their Internet development so as to realize its goal of advancing common and equitable development of cyberspace for all countries, thus infusing (injecting) impetus for their cyber capability-building to safeguard their cybersecurity.

For example, in 2009 China signed with ASEAN and Shanghai Cooperation Organization (SCO) respectively the China-ASEAN Coordination Framework for Network and Information Security Emergency Responses and the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, both of which have greatly promoted regional cooperation on cybersecurity issues. Of course, every country should join this international cooperation process in the future.

Third, China needs to enhance intra-governmental coordination. In other words, China needs to enhance the coordination between different governmental departments and strengthen its institutional capability building in cyber field.

Just like other countries, there are different departments in charge of different dimensions of cyber issues. The Ministry of Industry and Information Technology (MIIT) is more of a technical orientation, the Ministry of Public Security (MPS) has a focus on combating cybercrimes, while the Ministry of Foreign Affairs (MFA) is responsible for those diplomatic activities connected with cybersecurity. Other governmental departments also have their own function to perform.

It is natural that these different departments have different views, visions and perspectives on cybersecurity. Therefore, to harvest the potential benefits to the largest degree on the one hand and to maintain and safeguard cybersecurity on the other hand, effective coordination among these departments is not only needed but also a must in their daily work. Now, the good news is that the Central Leading Group on Cybersecurity and Informationization has been established, and is expected to play a central, leading and coordinative role in all aspects of cybersecurity in China.

Last but least, China should further promote international and bilateral cyber cooperation, which is an inalienable dimension of cybersecurity. Besides what has been said in the previous section, the following also deserves our attention.

In recent years, the international community has been calling for rules for cyberspace to be made, in the process of which all countries are indispensable. In particular, the United States and the West have been very active in an attempt to formulate cyber rules. In September 2012, Mr. Harold Hongju Koh, legal advisor of the U.S. Department of State, presented the U.S. views on international law in cyberspace during a USCYBERCOM Inter-Agency Legal Conference. In the same month, NATO also tabled its Tallinn Manual[28], exploring the applicability of the International Humanitarian Law (IHL) in cyberspace. Before that, in September 2011, China, Russia, Tajikistan and Uzbekistan also proposed a draft "International Code of Conduct on Information Security" at the UN General Assembly.

28 Michael N. Schmitt, (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare – Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyberdefence Center of Excellence*, Cambridge University Press, 2013.

Although China hoped the international community could have in-depth discussions within the framework of the UN Group of Governmental Experts on the Issue of Information Security and reach agreement at an early date, the draft proposal was "largely dismissed by Washington and its Western allies". However, just as Mr. Amitai Etzioni, a senior advisor to the Carter White House, said, "if one did not know which nations submitted this proposal, one could easily assume that 95 percent of the draft code was composed by Western nations led by the United States".[29] Therefore, China, a member of the developing countries, and the United States, a representative of the developed countries, have so many common interests in cyberspace that it is a must to initiate talks on the draft proposal, during which more common grounds could be found and deeper mutual trust be built.

As the Stuxnet worm against the Iranian nuclear facilities demonstrates, cyber tools and weapons could lead to catastrophic scenarios. Therefore, the international community could negotiate an agreement to constrain the research, development and use of cyber tools and weapons, drawing on the experiences of the conventions on nuclear, chemical and biological weapons. Though cyber tools and weapons are unique and hard to verify, limiting cyber weapons could become a new direction for international cyber negotiations. The international community could also step in this thorny field, contributing to international cyber peace and security.

Accordingly, China thinks that cyberspace should be used for peaceful purposes and every country and man should enjoy the enormous benefits brought about by the development of the Internet. The lessons and tragic

29 Amitai Etzioni, "China Might Negotiate Cybersecurity", *The National Interest*, March 14, 2013, http://nationalinterest.org/commentary/china-might-negotiate-cybersecurity-8222.

consequences of the two world wars should not be discarded, and therefore, the trend towards militarization and weaponization of cyberspace should be strongly resisted, given the great potential damage it could incur.

Since cyberspace is not an isolated realm immune from the influence of relations in other fields, e.g. political and economic relations, we often have to view their cyber relations from a perspective of overall bilateral or international relations. To safeguard the peace and stability of cyberspace, efforts to maintain good state-to-state relations in other fields are also needed. Although the West, particularly the United States, is keen on accusing China of the cyber-attacks it suffers, today they are in fact faced with common cybersecurity threats/interests.

Cyberspace is a new domain for security studies with many questions to be figured out. Despite the fact that China is one of the major victims of cyber-attacks, just as in other domains in international relations, China has once again become the default target for accusation when the West, particularly the U.S., tries to release its complaints and find a scapegoat for the cyber-attacks from which it suffers.

Though China's positions are crystal clear, the West seems to have formed a bad habit of accusing China whenever something unpleasant occurs. On the contrary, China has always embraced a modest, low-profile and even humble approach to foreign affairs, which is different from the bold, assertive, and even aggressive one of some other countries. China also advocates and practices an active defense policy, which is defensive rather than offensive in nature. This also applies to the new domain of cyberspace.

Given the difficulty in cyber-attack attribution, *inter alia*, the transnational and anonymous nature of cyber threats, it is neither professional nor responsible to make groundless

accusations without hard evidence and is also not conducive to solving relevant problems. That is why China seldom publicizes or blame others for the cyber-attacks it suffers, thereby a Chinese way of performing cybersecurity is in the making.

1.7. Conclusion

China is a latecomer to the cyber field, but it has achieved enormous progress in the development of the Internet. It sees Internet development as part of its great cause of reform, opening up and modernization. It has put forward and implemented active and vigorous policies towards the Internet.

China adheres to the principle of scientific and effective Internet administration by law. It has formulated an effective and overall system of Internet administration, which is a combination of laws and regulations, administrative supervision, self-regulation, technical protection, public supervision and social education.

China has promoted international cooperation on cyber issues in an active manner. It has conducted various strategic and security dialogues and consultations on cybersecurity with numerous countries, carried out legal cooperation on fighting against cybercrimes, engaged in technical cooperation in addressing cyber incidents on a daily basis, and so on.

China has not yet produced a cybersecurity strategy as of April 2014, but the international cybersecurity situation will make China think more about it. The establishment of the Central Leading Group on Cybersecurity and Informationization will add a new impetus to this process.

Given the interconnected nature of cyberspace, noone could go it alone. Therefore, to tackle increasing cybersecurity hazards, international cooperation is needed. Specifically, enhanced technical cooperation among experts will yield twice the result with half the effort; on the governmental level, all countries should reinforce mutual trust and share best practices and experiences; on the operational level, various organizations also need to work with each other as cyber threats are always transnational ones. In a word, new steps and thinking are needed to advance cybersecurity and to build a peaceful, secure, open and cooperative cyberspace. This is what China advocates and practices.

2

PLA Views on Informationized Warfare, Information Warfare and Information Operations

Over the course of the past two decades, the Chinese People's Liberation Army (PLA) has been closely examining the experiences of foreign militaries as it has sought to modernize itself and prepare for warfare under new, more high-technology conditions. Having not fought a war itself since 1979, the PLA nonetheless recognizes that the nature of modern warfare has fundamentally evolved in the intervening 35 years, and that it must adapt if it is to be victorious in future conflicts.

In the view of Chinese analysts, the advances in information technology have fundamentally altered the character of modern warfare. Consequently, an essential part of the PLA's approach to future wars is the need to secure "information dominance (zhixinxiquan; 制信息权)". This extends beyond the realm of computer network attack and defense, and instead encompasses not only information systems (both hardware and software), but also the cognitive

Chapter written by Dean CHENG.

and decision-making aspects of military and political command.

2.1. The evolution of chinese military thinking

Even before the end of the Cold War, the PLA had already concluded that reliance on massed numbers of ill-trained, poorly equipped troops was no longer appropriate. Chinese assessments of the American war in Vietnam and the "Fourth Middle East War" of 1973 indicate a recognition of the growing importance of technology in warfare. Weapons had greater reach, and significantly improved lethality. Of equal importance, surveillance and reconnaissance systems had improved capabilities, making them more significant in the calculus of effectiveness. The Sino-Vietnam War of 1979 further underscored the growing role of technology in modern warfare.

By the early 1990s, it was clear that high technology was affecting not only weapons, but tactical and even strategic outcomes. Modern weapons, as seen in the first Gulf War (1990-1991), shifted the emphasis from the destruction of opponents to paralyzing them, in the course of defeating them. Moreover, the new technologies also expanded the operating areas, so that land, sea, and air arenas were no longer the complete set of potential battlefields. The same information technologies and improved sensor systems that made modern weapons that much more destructive, effectively made information space and outer space key battlegrounds as well.

Meanwhile, the pace and destructiveness of modern wars was such that even local wars (i.e. those not involving the mass mobilization of the nation and the economy) nonetheless

could affect the entire country.[1] Warfare was much more non-linear in nature, shifting from primarily ground/sea centered, to an exploitation of all three dimensions. Of particular importance, airpower, including long-range bombers and air- and sea-launched cruise missiles, was now much more destructive and decisive. At the same time, warfare was much more intense, involving round-the-clock operations. This also meant that the sheer material expenditure of warfare was even more substantial, further increasing the importance of logistics and sustainability. All of these elements, marking what the Chinese considered to be a global military transformation, were encompassed in the idea of "Local War Under Modern, High-Tech Conditions". Preparing for such wars became the basis for PLA operational planning in a Jiang Zemin-issued directive to the Chinese Central Military Commission (CMC) in 1993.

In these directives, Jiang called on the PLA to undertake the "Two Transformations", in the course of modernizing. The first transformation was in the kind of war that the PLA should be preparing for; a shift from "Local Wars under Modern Conditions", to "Local Wars Under Modern, High-Tech Conditions". This, in turn, would require the PLA to transform from focusing on quantity, to emphasizing quality, and especially the incorporation of technology.

In 1999, the PLA issued a new series of thoroughly revised manuals and regulations that constituted the "New Generation Operations Regulations". These regulations embody and codify the two transformations that Jiang demanded of the PLA. They constituted a wholesale revision of operational doctrine, affecting every aspect of the PLA, from its conception of future wars to training and organization.

---

1 Gao Yubiao, Chief Editor, *Joint Campaign Course Materials* (Beijing: AMS Publishing House, August 2001), p. 45.

– The quality, as well as the quantity, of weapons matters. The side with more technologically sophisticated weapons would be able to determine the parameters of the conflict, and effectively control its scale and extent.

– The battlefields associated with such conflicts are three-dimensional, and extend farther and deeper into the strategic rear areas of the conflicting sides.

– The conflict is marked by high operational tempos conducted around the clock, under all-weather conditions.

– The fundamental approach to warfare is different. Such wars would place much greater emphasis on joint operations, while also incorporating more aerial combat, long-distance strike, and mobile operations.

– Finally, the role of command, control, communications and intelligence is paramount. C3I functions were seen as essential to successful implementation of such wars; consequently, the ability to interfere with an opponent's C3I functions also became much more important.[2]

Analysis of more recent subsequent conflicts has further complicated PLA planning. NATO operations in the Balkans, the toppling of the Taliban in Afghanistan, and the second Gulf War have led PLA analysts to conclude that "Local Wars under Modern, High Tech Conditions" have now transitioned to "Local Wars under Informationized Conditions". In these wars, command, control, communications, and intelligence (C3I) assumed ever growing prominence.

2 Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia*, Vol. II, (Beijing, PRC: Academy of Military Science Publishing House, July 1997), pp. 126–127.

The ability to apply airpower effectively required coordinating air forces with land and naval forces. In short, the PLA must be able to conduct joint operations, in order to be able to win future wars. This, in turn, imposed significant demands upon command, control, communications, and intelligence functions. Successful joint operations require, at base, the ability to coordinate forces that operate across the various domains, and the ability to create a shared sense of situational awareness. Consequently, by the 1990s, the PLA recognized that they had to master the ability to bring together, land, sea, and air forces, and be able to operate in the land, sea, air, outer space, and information space domains. Airpower was increasingly seen as an essential tool, enabled through the ability to control the nature and flow of information.

Again, the senior leadership codified this shift by giving new guidance to the PLA. Hu Jintao, in his role as Chairman of the Central Military Commission, issued "new historic missions" to the PLA. According to Hu, the PLA would be responsible for:

– defending the Party's hold on power;

– providing conditions for national economic development;

– furthering world peace through UN/peacekeeping interactions;

– most relevant here, preserving Chinese interests, especially in the maritime, space, and cyber domains. These are the essential domains for future Local Wars under High-Tech Conditions, and what the Chinese now term Local Wars Under Informationized Conditions.

2.2. The growing importance of information

As PLA authors note, wars reflect the broader state of societal and industrial development. Thus, as society has

evolved from the Industrial Age to the Information Age, its wars have shifted from mechanized warfare to informationized warfare (*xinxihuazhanzheng*; 信息化战争). In such wars, information and knowledge are core resources, and the resulting broad use of information technology allows the creation of a single, integrated information-space within which participating forces operate.

Informationized wars, not surprisingly, require informationized militaries, forces where information is integrated into each and every function – not just the weapons and their employment, but also logistics, personnel management, command and control. Only in this manner can there be real-time sharing and exploitation of information, to maximize its effect on operations. Only informationized forces can have fully developed integrated strength, drawing upon the capabilities of all the participating services and exploiting their respective strengths, while shielding each of their weaknesses.[3]

Informationized warfare, then, is in many ways a conflict between rival systems-of-systems. Each side seeks to create an integrated situational picture, and best exploit their respective capabilities. At the same time, since a system requires the smooth interoperation of all of its subordinate systems and sub-systems, an essential part of informationized warfare is striving to prevent that smooth interoperation. Thus, informationized warfare will involve attacking the key nodes and links within the other side's system-of-systems, to precipitate cascading failures.

While informationized warfare is the *application* of information technology across the full range of military

3 AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Information Operations Theory Study Guide* (Beijing, PRC: AMS Publishing House, 2005), pp. 42–43.

activities, information war (*xinxizhan*; 信息战) involves making *information itself* the focus of warfare. Within this concept, information collection, management and analysis, transmission and exploitation are some of the main operational techniques. The focus is on disrupting the enemy's information, information systems, and information users, while defending one's own. The side that is best able to do this is able to secure the "information advantage (*xinxiyoushi*; 信息优势)".

In the Chinese view, information war (sometimes also translated as "information warfare") has both a broad and a narrow meaning. The broad meaning of information war can also be termed "strategic information war", which refers to the two sides' use of information and information technology in the political, economic, S&T, diplomatic, cultural, and military arenas in order to secure information advantage. In this broad sense, information war spans military and civilian spheres, peacetime and wartime, and has a global nature. Strategic information war is an ongoing process.

The Chinese interest in "political warfare", including public opinion warfare, psychological warfare, and legal warfare, is an example of "strategic information war". It targets not just information *per se*, to fundamentally influence the context and framework of information. Strategic information war is aimed at influencing how information is perceived and interpreted, by not just military audiences, but the opponent's civilian population, top leadership (military and civilian), and also third-party governments, militaries, and civilian populace.

The narrow meaning of information war involves the two sides in wartime driving to secure the information advantage, and undertaking information conflict, primarily in the military arena. As the Chinese note, this is what the US terms "battlefield information warfare". The narrow form of information war targets the C4ISR systems, degrading the

enemy's and protecting and preserving one's own. It builds upon the use of electronic technology as a support for electronic warfare (i.e. electronic warfare is the foundation), and its core remains electronic warfare.[4]

The main goal in information war, especially in the narrow sense, is securing "information dominance (*zhixinxiquan*; 制信息权)". This is consistent with other PLA writings, which emphasize the importance of establishing "space dominance", "air dominance", and "maritime dominance".

Information dominance refers to the ability to establish control at a given time and space over battlefield information, while denying an opponent the same. In this context, battlefield information refers to information relating to the activities and changes in friendly and enemy forces, as well as the physical conditions of the battlefield (e.g., weather).[5] Information dominance is generally seen as a temporary condition; it is difficult, if not impossible, to create a permanent condition of information dominance, unless one side enjoys an overwhelming advantage.

Establishing information dominance requires targeting and protecting information collection, management, and allocation assets; the communications and data links involved in getting information from sensors to users; the users themselves, including the decision-makers, commanders, weapons systems, and their controllers); and

4 AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office,*Information Operations Theory Study Guide* (Beijing, PRC: AMS Publishing House, 2005), pp. 67–69.

5 AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Information Operations Theory Study Guide* (Beijing, PRC: AMS Publishing House, 2005), pp. 13–14.

the information itself. One of the key targets is the decision-maker. Isolating them, destroying them, influencing and undermining them, are all elements of establishing information dominance.

In this regard, the Chinese are engaging in the obverse of what the NATO forces sought to do in the 1980s. For NATO, the purpose was to get inside the OODA loop of the Soviet adversary, to be able to engage in the OODA chain faster than their Soviet counterparts. At this point in time, the Chinese do not seem to think that they can be faster, so securing information dominance involves slowing down the opponent's OODA loop.

Because of the importance of information in informationized war and information war, information dominance is seen as the prerequisite for establishing dominance in other domains, including sea, air, and outer space. As important, establishing information dominance includes operations in these other domains, because it entails not only things like cyberwarfare, but also the physical destruction and degradation of enemy information systems, such as command posts and communications systems. It therefore includes firepower strikes, special operations forces activities, as well as electronic and computer network warfare operations.[6] Conversely, establishing air or space dominance facilitates establishing information dominance. In particular, space capabilities are seen as intimately linked with informationized war and information war – space will be a key battleground in the struggle for information dominance.

Information dominance is rarely absolute. Instead, the initial focus should be on establishing it at key times and

6 Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), pp. 179–185.

places, or denying it to an enemy at those essential periods. The expectation is that the struggle for information dominance will be constant, lasting throughout the course of a conflict. This, in turn, means that there are different means that might gain or lose importance over that period. Thus, at one point, it might mean affecting decision-makers; at another, it might involve computer network attack.

2.3. Information operations

Information war (*xinxizhan*; 信息战) involves campaigns and battles in pursuit of information dominance. Information operations (*xinxizuozhan*; 信息作战) are focused on specific activities and operations aimed at securing and maintaining information dominance, in terms of friendly and adversary attempts to be able to freely collect battlefield information.[7] Information operations refers to those activities that seek to disrupt the enemy's information and information systems, influence their ability to exploit information, while preserving one's own abilities in this regard.

Information operations are guided by the concept: "information as the main guide, offense and defense both prepared, network and electronic [warfare] unified, systems mutually accommodating [or linked] (*xinxizhudao, gongfangjianbei, wangdianyiti, xitongjianrong*; 信息主导，攻防兼备，网电一体，系统兼容)".[8] PLA writings suggest that all forms of information operations are likely to include aspects of electronic warfare (*dianzizhan*; 电子战),

7 Tan Rukun, *Teaching Materials on Operational Strength Construction* (Beijing, PRC: AMS Publishing, 2011), pp. 196–197, and Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), p. 2.

8 Tan Rukun, *Teaching Materials on Operational Strength Construction* (Beijing, PRC: AMS Publishing, 2011), p. 202.

computer network warfare (*wangluozhan*; 网络战), and psychological warfare (*xinlizhan*; 心理战). Computer network warfare, or cyberwarfare, then, is not the only type of information operations, nor even the most important; rather, it is integrated into this broader conception of seeking to secure information dominance, and works in conjunction with electronic warfare (sometimes described as integrated network and electronic warfare) and psychological warfare.

The concept of information operations covers four broad mission areas in Chinese analyses; as presented in the following sections.

2.3.1. *Command and control missions*

First and foremost is the ability to exercise command and control over one's own forces. This entails the ability to collect, transmit, and exploit information. It requires commanders and staffs who can operate consistent with the operational plan, and whose decisions are not adversely affected by enemy propaganda, enemy influence, or enemy perception management. The struggle to be able to implement effective command and control in the face of electronic warfare, computer network warfare, and psychological warfare has given rise to what some Chinese analysts term "command and control warfare".

Effective exercise of command and control, in light of advances in information technology, should allow for a flatter command and control structure, as well as a greater reliance on "mission oriented orders". Commanders are expected to think one level higher, when setting objectives, consistent with their understanding of the overall objectives of campaigns.

2.3.2. *Offensive information missions*

Offensive information operations (*xinxijingongzuozhan*; 信息进攻作战) are essential for obtaining information advantage and establishing information dominance, since we cannot achieve information dominance solely through defensive measures. The PLA envisions several different means of implementing offensive information missions, including information coercion, information blockade, creating an information advantage, information contamination, and information paralysis, in each case combining various techniques including electronic warfare, computer network warfare, psychological warfare, and physical attacks.[9]

2.3.2.1. *Information coercion / information deterrence*

The Chinese term for "deterrence", *weishe* (威慑), can also be translated into "coercion". In the case of information operations, PLA writings suggest that we may be able to coerce an opponent through displays of information attack capabilities, including electronic interference and computer network attacks. PLA writings suggest that information coercion should be implemented in coordination with conventional and even nuclear measures. Thus, electronic interference should be undertaken at times that might mask other conventional force deployments, to induce confusion in the opponent's camp.

Similarly, information coercion methods should be coordinated with public opinion warfare techniques, so that the threat is publicized to senior political leaders and the broader populace. Ideally, an information coercion effort would lead to degraded adversary information systems,

9 Drawn from Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), pp. 109–114.

confusion about overall Chinese capabilities, and a general lowering of adversary morale as a consequence.

In the Chinese view, information coercion methods have the advantage that they are more credible than conventional military or nuclear deterrent/coercive methods. The various methods involved in such an effort need not be formally acknowledged, and may not directly damage an opponent's physical or data infrastructure, while nonetheless applying psychological pressure against their key military and civilian decision makers.

2.3.2.2. *Information blockade*

An information blockade involves large-scale suppression and interference with an adversary's electronic and information systems. It includes not only electronic interference measures such as jamming, but also electronic deception and computer network penetration, to effectively cut an opponent's ability to communicate with the outside world. It also involves efforts to prevent an opponent from obtaining information about the outside world; so, information blockades may also incorporate such steps as radar jamming, blinding or dazzling of reconnaissance satellites, and even physical destruction of reconnaissance aircraft and other information gathering systems.

According to PLA analysts, information blockades can be difficult to impose, because of the myriad ways that we can obtain information. Consequently, sequencing one's information blockade efforts, such as by attacking terrestrial communications systems and then jamming radios, is essential. For the same reason, any information blockade will likely require the application of many different methods, and cannot rely on just computer network attack or jamming.

2.3.2.3. *Information misdirection.*

Information misdirection (*xinxizaoshi*; 信息造势) involves employing various means, including electronic and computer network deception, decoys, false information, etc., to manipulate an opponent's perceptions, thereby misleading them regarding one's own capabilities, intentions, and actions, and creating the opportunity for surprise. With the PLA's longstanding interest in the application of deception and stratagem, information misdirection is the merging of such techniques with modern information technology.

As with any misdirection effort, information misdirection must be integrated into the overall strategic and operational plan. Troop movements, air and missile strikes, other communications should all be consistent with the misdirection effort. At the same time, information misdirection efforts should be consistent with realistic military goals. The Chinese assessment resembles the Allied effort to conceal the invasion at Normandy by emphasizing Calais, which played to the Germans' firmly held belief that any invasion would have to seize a port.

To this end, information misdirection efforts must be comprehensive, and cannot rely on a single source or method. As PLA analysts note, the misleading information must be capable of fooling the enemy's battlefield reconnaissance systems, their intelligence agencies and departments, and the other side's commanders. This can only occur if the false information is independently corroborated, which in turn requires many different strands of mutually supporting false information. They must also incorporate defensive measures, to ensure that one's misdirection plans are not leaked or otherwise discovered by an adversary.

2.3.2.4. *Information contamination*

Information contamination efforts involve the deliberate introduction of false, useless or infected information into the enemy's information systems. The goal is to degrade an opponent's ability to transmit information, disrupt their ability to use information, and infect their information systems, so that their information processing and exploitation capacities are crippled.

Information contamination efforts include denial of service attacks and introduction of computer viruses and logic bombs into opposing computer networks, but extend further, to include attacks on the enemy's entire communications network, including both land-lines (e.g. fiber optic cables) and wireless systems, and information misdirection methods, to overwhelm an opponent with a flood of false information. They also include physical measures to obstruct or confuse enemy reconnaissance systems, so that the intelligence collected is incomplete or misleading.

2.3.2.5. *Information paralysis*

The PLA also discusses the need to paralyze an opponent's information collection, transmission and management systems, through electronic, physical and other attacks. This goes beyond denying an opponent information (as in an information blockade), to actively destroying and disrupting their information systems. As one PLA analysis notes,

> This means concentrating information attack troops and weapons, and undertaking electronic interference, [computer] virus attacks, and firepower strikes against enemy information systems, especially specific key elements (such as nodes). This will reduce and

> disrupt the integrated operational effectiveness of enemy information systems.[10]

Information paralysis efforts will entail both hard kill and soft kill methods, and employ electronic means, firepower strikes from land, sea, and aerial platforms, and also employ special operations forces. They will focus on command centers and command posts, as well as key sub-systems, including battlefield early warning command and control structures, main routers and switching centers of the telecommunications system, and radar networks and associated communications links. In the Chinese conception, once such systems are successfully attacks, an opponent's command and control system will be unable to function normally, and will become paralyzed.

2.3.3. *Defensive information missions*

Defensive information operations (*xinxifangyuzuozhan*; 信息防御作战) complement offensive information operations. They are aimed at maintaining information resources, shielding them from enemy interference and restoring them, should they nonetheless be disrupted. This includes concealment, camouflage and deception, deterrence, early warning, and crisis response.[11]

– *Information concealment* includes both physical concealment, camouflage, and deception (CCD), but also electronic concealment measures. Part of this is aimed at preserving the physical infrastructures and facilities, but also preventing information leaks. The goal is to prevent an

10 Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), p. 114.
11 Tan Rukun, *Teaching Materials on Operational Strength Construction* (Beijing, PRC: AMS Publishing, 2011), p. 202.

adversary from obtaining information about one's own information networks and systems.

– *Information deterrence* refers to the use of international law, diplomatic conflict, and potential retaliation techniques to make the enemy reduce or entirely lose their interest or capacity to undertake information attacks. This would apply to legal warfare and public opinion warfare techniques, aspects of "political warfare".

– *Early warning* provides the opportunity for Chinese forces to detect signs of an impending attack, and allow for the activation of back-up information system, creation of pristine copies, etc. The goal is to minimize the impact of enemy information offensive operations, and might also contribute to information deterrence. In the Chinese view, if they can make clear that an opponent's information offensive has already been detected, the adversary may choose not to proceed. Similarly, if previously existing vulnerabilities in Chinese electronic systems are suddenly neutralized, an adversary may decide that it should delay action, and perhaps even avoid conflict altogether.

– Early warning works intimately with *information crisis response preparations*. This includes physical dispersal and redundancy. Chinese analysts emphasize that information systems need to be networked, so that attacks on any given node or element will not necessarily collapse the system. In the event of a crisis, additional information resources may be activated, while civilian and commercial assets may be mobilized.

2.3.4. *Information support and safeguarding missions*

Mechanized warfare mainly involves the expenditure of steel, explosives, material instruments, and manpower. Informationized warfare, aside from these expenditures, also emphasizes the large demands for information and the

large-scale consumption of information-related systems. In informationized operations, the two sides will not only be engaged in a contest between information offense and defense capability, but will also compete in logistical support capacity for those information operations. In the complex electromagnetic environment, it is necessary to ensure the smooth operation, and replacement when necessary, of electronic warfare equipment, information networks (including their physical facilities), and command networks. The battlefield commander needs geographic survey information, meteorological and hydrographic information, as well as civilian information resources, etc., which is also part of the responsibility of information safeguarding work.

2.4. Key types of information operations

In order to fulfill these broad mission areas, PLA analysts believe that future military forces must be able to engage in specific types of information operations. The most important are electronic combat, computer network combat, psychological warfare (including deception), but also include intelligence combat, command and control strength, and physical destruction.

2.4.1. *Electronic combat (dianzizhan; 电子战)*

Electronic combat is a subset of the larger array of information operations. It refers to the capacity to attrit and disrupt the enemy's electronic equipment, while defending one's own electronic facilities and systems, and their normal operational capacity. Electronic combat is linked to computer network combat, but is more focused on electronic systems, and not solely those relating to information collection and

transmission, or computer systems. In the PLA's view, it is the foundation for broader information operations.[12]

Electronic combat includes electronic reconnaissance, measurement and signature intelligence, computer network reconnaissance, and electronic information management and security. It includes electronic offensive and defensive measures, and can incorporate physical as well as electronic measures.

2.4.2. *Network combat (wangluozhan; 网络战)*

Network combat, or computer network combat, refers to those operational activities that employ computer network facilities, and the undertaking of computer network reconnaissance, offensive, and defensive missions. The goal of network combat is to establish network dominance (*zhiwangluoquan*; 制网络权) by attacking enemy computer networks and the information that passes over them.

It includes, on the one hand, any effort aimed at disrupting information networks, whether by nations, sub-national groups, the broad population (e.g. "patriotic hackers"), or terrorists. More narrowly, it refers to the range of information operations involving computer networks that are aimed at securing network dominance by attriting or disrupting the enemy's computer networks systems' information and ability to operate, while ensuring that one's own computer network systems' information and security.[13] Network combat can therefore entail operations against

12 AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office,*Information Operations Theory Study Guide* (Beijing, PRC: AMS Publishing House, 2005), p. 94.
13 Tan Rukun, *Teaching Materials on Operational Strength Construction* (Beijing, PRC: AMS Publishing, 2011), p. 204.

computer hardware, computer software, as well as data passing over the computer network itself.

Network combat can be divided into strategic network combat and battlefield network combat.

Strategic network combat refers to the use of the Internet to attack the enemy's national political, economic, military, cultural, diplomatic, and other information basic facilities, attriting the enemy's strategic information resources and ability to employ information. We seeks, through network conflict activities to attrit the enemy's comprehensive national power, while at the same time protecting one's own strategic information facilities, information resources, and information capability.

Battlefield network combat is the narrow meaning of network combat. It involves network attack, network defense, and network support operations and missions, as conducted by information operations units (*xinxizuozhanbudui*; 信息作战部队).

2.4.3. *Psychological combat (xinlizhan; 心理战)*

From the Chinese perspective, the human element is as much part of information warfare as the digital or physical elements. Consequently, information operations include a large component of psychological warfare.

The goal of psychological combat, in the context of information operations, is to influence the perceptions and thought processes of the two sides' decision-makers and information users. It involves the employment of various types of information, delivered through such means as news media, social media, public opinion, to influence an adversary's emotions, perspectives, concepts, attitudes, so as to reduce their spirit and will, and disrupt their

psychological balance, shaking their willingness to fight.[14] There is also an element of disrupting their cognitive functions, whether through information overload or the imposition of psychological pressures, so as to lead to poor judgments and reduced combat effectiveness.

Psychological combat can occur at the strategic, operational, and tactical levels of war. Such efforts include emotional appeals, intimidation (such as warnings sent to the private accounts of senior officers and political figures), deception, and the spreading of defeatist attitudes. These efforts can be implemented through such means as social media and Internet memes, as well as more traditional broadcasts, leaflets, etc.[15]

Psychological defensive measures not only seek to neutralize enemy information attacks, including psychological attacks, but also to break any enemy attempts at imposing an information blockade, which creates a sense of isolation and helplessness. This is one lesson the Chinese seem to have derived from the two Gulf Wars, that the imposition of an "information blockade" can have devastating psychological consequences.

2.4.4. *Intelligence combat (qingbaozhan; 情报战).*

Intelligence combat (*qingbaozhan*; 情报战) is an essential element of information warfare and information operations. It involves efforts to collect intelligence information, control its flow, and apply it more effectively than an opponent, while at the same time defeating their efforts to obtain and

14 Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), pp. 14–15.
15 Xie Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: AMS Publishing House, 2013), pp. 179–180.

exploit intelligence. Intelligence combat is ultimately focused on the collection of information.[16]

Intelligence combat has a broad and a narrow meaning. The broad meaning refers to the effort by the antagonists to collect information pertaining to politics, economics, science and technology, as well as military, cultural, and diplomatic aspects. The narrow meaning of intelligence combat refers to the efforts to secure or counter the securing of military intelligence. In each case, there are strategic, operational, and tactical dimensions.

It should be noted that even under the narrow meaning, intelligence warfare includes broad aspects of information collection, such as of meteorological and hydrologic information and space situational awareness so as to better understand likely battlefield conditions. Similarly, it involves the creation of electronic and physical orders of battle, accumulating libraries of electronic and acoustic signatures and characteristics.[17] Because such information can only be acquired over an extended period of time, intelligence combat is a constant effort that overlaps the boundaries between peace and war.

2.4.5. *Command and control combat (zhihuikongzhizhan; 指挥控制战)*

Command and control combat (*zhihuikongzhizhan*; 指挥控制战) is the struggle by the two sides in a conflict to secure an advantage in the exercising of command and control over one's forces. It involves preserving one's own command and control networks, while disrupting and destroying the enemy's. Command and control warfare

16 Li Naiguo, *New Concepts of Information Warfare* (Beijing, PRC: AMS Publishing House, 2004), p. 35.
17 Sung Yuejin, *Command and Control Warfare* (Beijing, PRC: National Defense Industry Press, 2012), pp. 29–30.

involves the comprehensive coordination of operational security, military deception, as well as electronic, network, and psychological warfare.[18]

In the Chinese conception, command and control combat is distinct from computer network combat, highlighting a fundamental difference between PLA and western military thinking.[19] Computer network combat is mainly undertaken by breaking into networks, engaging in electronic recon, breaking into (storage) media, in order to gain network information, and obtain local network superiority (*jubuzhiwangluoquan*; 局部制网络权). Command and control warfare mainly focuses on disrupting command and control network operations, affecting and attriting enemy command and control system effectiveness, so that the enemy's command and control systems are paralyzed or suffer temporary breaks. Chinese writings imply that this focus is on military C2 systems, which would suggest that SCADA-type attacks would be part of computer network, rather than command and control, combat.

To a particular degree, it may be said that command and control combat is a special type of computer network combat. Command and control strength refers to the command and control information systems at command centers (*zhihuizhongxin*; 指挥中心), and the associated command posts (*zhihuisuo*; 指挥所), as well as the facility systems and workers at command terminals (*zhihuizhongduan*; 指挥终端), who employ command and control information systems, in the process of exercising operational command, in future information operations or joint campaign operational activities (*weilaixinxizuozhanhuolianhezhanyizuozhanxing dong*; 未来信息作战或联合战役作战行动). Command and control

18 Sung Yuejin, *Command and Control Warfare* (Beijing, PRC: National Defense Industry Press, 2012), p. 29.
19 Tan Rukun, *Teaching Materials on Operational Strength Construction* (Beijing, PRC: AMS Publishing, 2011), pp. 205–206.

combat, then, will incorporate computer network attack aimed at those command centers and command posts, and efforts to defend one's own facilities. However, it will also encompass physical attacks aimed at those facilities as well.

2.4.6. *Physical combat*

Just as information operations include psychological efforts aimed at the human factor, it also includes physical attacks against the various components of the opponent's command, control, and information networks. Consequently, PLA writings note that physical attacks, by the range of military systems, from ballistic missiles to aircraft to special operations forces, are also an essential part of information operations.

PLA analyses note that physical attacks can often have synergistic effects, complementing other forms of information operations. In the 1979 Sino-Vietnamese War, for example, it is noted that Chinese forces targeted Vietnamese artillery communications land-lines, compelling artillery forces to rely on radios to communicate with spotters and observation posts. The Chinese then employed jammers and other methods to disrupt the radio-links, neutralizing coordination efforts.[20] We can posit similar effects through, for example, the destruction of enemy reconnaissance aircraft which may compel reliance on predictable satellites. Conversely, destroying satellites may eliminate wide-coverage surveillance capabilities which can only be partially compensated through aircraft.

Physical attacks can also provide windows of opportunity. We need not destroy an entire constellation of observation satellites, it may be sufficient to simply create periods of

20 Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: NDU Publishing House, 2009), p. 111.

blindness. Similarly, because information dominance is difficult to maintain over the entire course of a conflict, physical attacks may create conditions of local superiority, or cause the enemy to withdraw or limit their information collection efforts (in order to preserve their own resources).[21]

2.5. Computer network warfare and information operations

All of this suggests that, for the Chinese People's Liberation Army, computer network reconnaissance, computer network attack, computer network defense, and computer network exploitation are not necessarily seen as stand-alone operations, but are integral to the broader tasks of information operations. Thus, computer network operations are part of command and control combat, psychological combat, and intelligence combat, as well as network combat.

This suggests that Chinese computer network operations need to be analyzed in the context of larger military operations. Given the Chinese emphasis on coordination, it is likely that their computer network operations will be coordinated with planned physical attacks in the land, sea, air, and outer space domains. Peacetime operations are likely intended to benefit wartime operations, whether by reconnoitering command and control structures, identifying key command and communications nodes, or influencing military and political decision-makers.

Conversely, it should be expected that Chinese efforts at computer network security are likely coordinated with other aspects of information security, including the civilian sector. Indeed, one Chinese analysis observes that computer

21 Xie Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: AMS Publishing House, 2013), p. 189.

"networks have become the front line and main staging ground for military information security efforts".[22] Chinese efforts in this regard likely benefit from both the outsize role of the government in Chinese cybersecurity (the so-called "Great Firewall of China"), and the extensive integration between military and civilian information networks.

22 Guo Ruobing, *Discussions of Military Information Security* (Beijing, PRC: NDU Publishing House, 2013), p. 66.

3

China's Adaptive Internet Management Strategy after the Emergence of Social Networks

China's central government welcomed, to some extent, the development of new information and communications technology within the national territory because it is seen as necessary for the economic development and opening up of the country, which remains the very top priority of the Communist Party of China (CPC). Beijing had no other choice but to accept the Internet within its borders, although it represented a political risk from the moment it was first introduced in the early 1990s.

The development of the Internet in China was fast-paced, growing from 22.5 million users in early 2001 to more than 500 million 10 years later (official estimates). In a country dominated by state-owned media, the Internet quickly became the main source of information and discussion for the most connected part of the population (most often the urban middle class). Tricks such as the use of proxies for

Chapter written by Alice EKMAN.

bypassing the Great Firewall, the main censorship instrument, became well-known among the younger part of Internet users.[1] Posting videos, online comments, and updating personal blogs became a popular daily practice for many users. In this context, the CPC constantly tried to adapt its censorship tools to the latest technological developments, and succeeded to a certain extent in keeping control of the Web.

This chapter considers – from a non-technical viewpoint – the overall development of the Internet and social networks in Mainland China from the early 2000s up to January 2014, and analyzes in particular how the central government in Beijing adapts to these developments, with the constant aim to maintain social and political stability. A particular emphasis is placed on recent years, taking into account decisions taken by the second mandate of Hu Jintao (2007-2012) and the new challenges that the new leadership led by Xi Jinping is currently trying to address. In this aim, latest official communications and press releases on Internet management are analyzed in depth.

This chapter leads to a broader reflection on the domestic political consequences of the development of social networks in a non-democratic regime, both from the perspective of Internet users and government.

3.1. Weibo: the turning point

3.1.1. *Adaptive behaviors*

In the late 2000s-early 2010s, the development of social networks and in particular Weibo, a Twitter-like platform

1 Circumvention strategies for crossing the Chinese firewall are well known, as Jonathan Benney recalls, "The Great Firewall of China", China Policy Institute Blog, November 3, 2013, http://blogs.nottingham.ac.uk/chinapolicyinstitute/2013/11/03/the-great-fearwall-of-china/.

which quickly became the most popular of the dozen Chinese language social networks available, marked a turning point for the Chinese authorities.[2] Weibo in itself represented – by the number of its users, the functions of the platform (messages limited to 140 characters, which can carry a substantial amount of information, Chinese being a dense language) and the speed with which it can propagate a message – a political challenge that never existed previously in China. It became a new platform of debate, enabling the expression of diverging views collectively. Key opinion-makers in China are leading bloggers and Weibo users with millions of followers. It is through Weibo that many scandals arose (corruption cases involving local officials, accidents, food safety and pollution cases, etc.), as local witnesses are providing online information unavailable in the state-owned media. In mid-2011, the mishandling of a high-speed train accident by the authorities in charge near Wenzhou, in the southeastern province of Zhejiang, was highly commented upon online, to such an extent that censors have been struggling to keep up with angry comments. At the time, a new practice developed among Internet users: some of them converted themselves into journalists by posting online photos taken on the site of the accident and reporting the latest developments at a faster pace that state-owned media did. It is also through Weibo and other social networks that many protests were launched, coordinated and amplified, leading to street gatherings and demonstrations. In general terms, social networks comparatively gain more weight in China than in countries with an independent media landscape.

2 Jonathan Benny recalls that initially SinaWeibo was a quasi-official microblog service, but that the rapid escalation of its use to cover public events and its nationwide popularity may have taken the state by surprise. Benney, Jonathan, "The Great Firewall of China", China Policy Institute Blog, November 3, 2013, http://blogs.nottingham.ac.uk/chinapolicyinstitute/2013/11/03/the-great-fearwall-of-china/.

In this context, and with Weibo remaining very popular, new platforms such as Weixin emerging and the Internet no longer being confined to an urban and educated public, the government has to learn how to deal with the Internet in the most efficient way according to its two-fold aim of domestic political stability and economic development. Shutting down the platforms is not an option, given their popularity and their economic benefits. Moreover, the rigid censorship and repression used towards traditional media and Web 1.0 pages is not always efficient in the current Web 2.0 era providing a large amount of user-generated content.

The authorities therefore adapt: they continue to use traditional means of control (Great Firewall, blocking of content with "sensitive keywords", closing of accounts, etc., in close cooperation with local Internet companies), but are now combining these automated controls with a case-by-case human and flexible approach on the ground depending on the risk of propagation. For instance, several groups of protesters against the construction of paraxylene (PX – a potentially harmful chemical) factories in Dalian (August 2011), Ningbo (October 2012) or Kunming (May 2013), finally won part of their case against the authorities as the protest became popular online and in the streets.

The protests in the Arab world from 2011 certainly reinforced Beijing's consciousness of the power of the Internet, and the importance of taking the social network "threat" seriously and promptly. Shortly after the rise of protests in Egypt, the Chinese authorities were concerned about online activists' calls for a similar revolution in China. A "Jasmine revolution" did not develop at national scale, which the police managed to contain through traditional on-line censorship and a heavy presence in cities where

demonstrations were to be organized.[3] But such events led Beijing to fine-tune its management of the Internet.

After the Arab spring events, Chinese authorities modified their approach towards social media, taking into closer account a wider set of online protests, even minor ones (there is no "small crisis"), reducing reaction time and adapting the type of response – rigid repression or flexible control,[4] contrary to some other authoritarian states – according to the case-by-case risk of nationwide propagation. Indeed, the party most of all fears the rapid nationwide spread of discussion of unpredictable events over social media. As a matter of fact, Beijing's management of the Internet has became flexible in recent years: strong online access restrictions are implemented when the risk of nationwide propagation of some criticism is high, but some degree of tolerance exists for the numerous online criticisms against specific, localized issues, which may not turn to a more general call for political system change. Cutting off access completely would be counterproductive, as it would generate strong Internet users' dissatisfactions, as well as generate economic loss.

Exceptionally, in the most sensitive place and time, the Internet has been partly or completely shut down in some provinces such as Tibet or Xinjiang. Such strict decisions reminds us that simple, technical options are in the hand of the authorities to limit suddenly the political risks attached

3 On the topic, see for instance YANG, Guobin, "China's Gradual Revolution", Opinion pages, The New York Times, March 13, 2011, http://www.nytimes.com/2011/03/14/opinion/14Yang.html?_r=0.

4 King, Roberts and Pan show that human, manual censorship is large in scale and complex, varying between areas and date of posting (for instance, it is particularly strong during major events such as the 2008 Olympic games). King, Gary, Jennifer Pan, Margaret E Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review 107/2* (May): 1–18.

to the Internet[5]. But this last resort option has never been used at national level, and when imposed locally, being offline in a digital age leads to several economic or social costs which can quickly contradict the strategy of economic development and social cohesion that the central government tries to implement, in particular to calm down ethnic tensions in provinces considered as sensitive. Positive or negative consequences on the economy are usually taken into consideration by the government before it takes decisions regarding management of the Internet (see section 3.2, page 89).

Social networks also force the CPC to reconsider its decades-long communication habits and adapt to the new media landscape. So far the traditional state-owned media such as the People's Daily or the national TV news bulletin on CCTV remain unchanged both in style and content – spreading official discourse and showing the leaders' meetings and achievements under a positive light. But these traditional media are regarded with greater cynicism both in light of the Web 2.0 era and the proliferation of both online and print media sources that provide increasingly in-depth reporting.

In addition, the traditional opacity that has surrounded China's political system since the creation of the People's Republic of China becomes an issue for the CPC in the Web 2.0 era. For instance, the silence surrounding the Bo Xilai case throughout 2012 or the public disappearance of the General Secretary-in-waiting for a duration of 2 weeks in September 2012 generated an online "wind of rumors" on internal party infighting and coup d'Etat attempts that Beijing had trouble clearing up. Hypotheses and guesses posted on the Internet are proportionate to the existing lack

5 On this topic, see for instance : "Behind China's Cyber Curtain – Visiting the country's far reaches, where the government shut down the Internet", Christopher Beam, New Republic, December 5, 2013.

of information, which often applies to the most sensitive domestic political issues such as intra-party tensions or CPC leaders' wealth.

However, it would be incomplete to only regard the Internet as a threat for the CPC and the political stability – or "harmonious society" (*hexie shehui*) – it is trying to maintain. The Internet is also, and increasingly, used by the CPC as a political communication tool.

3.1.2. *Participative behaviors*

Ministers and other senior officials are conducting online interviews and chat sessions on the Internet versions of state-run media,[6] while several ministries and central government institutions are encouraged to develop online communication campaigns toward the local population and public diplomacy toward foreign audiences (the Ministry of Foreign Affairs has its own Weibo account, for instance). Beijing now tolerates – to some extent – online denunciation of local corrupted officials, and since the 18th Party Congress, social networks spread family pictures of Xi Jinping in an attempt to make the new leader appear closer to the people. A new form of online Party propaganda is emerging to influence and guide Chinese users (through online informal pro-CPC comments for instance)[7], attenuate

6 For instance, in 2010-2011, during the time he was Prime Minister, Wen Jiabao went online several times to talk with Chinese Web users, in an attempt to demonstrate his awareness of pressing social issues and appear close to the people.

7 From the mid-2000s, the central and local governments started to encourage public comments in favor of the Party, through small financial compensations. Such Internet commentators are known as the "50 Cent Party" (五毛党), because they are said to receive 50 cent of RMB for each online post supporting the Party line, or contradicting previous anti-Party posts. This is part of the government's new "public opinion guidance" strategy.

rising scandals and try to rebuild part of the lost legitimacy of the Party.

The Internet is not only a new propaganda field but also an instrument of analysis and forecasting. It helps the CPC to anticipate crisis and social unrest, not only by facilitating the collection of information on dissidents, but also by helping to understand trends in public opinion.

In order to avoid the risk of online unrest (potentially leading to offline unrest), the CPC reinforced what its Internet management strategy, which includes the prevalence of strict, traditional censorship, the uses of online propaganda (both traditional, and "smart", involving grass-root pro-CPC comments) as well as the development of a very sophisticated network of public opinion monitoring (polling, online comments analysis and synthesis), conducted throughout the country. Indeed, the most significant development in recent years is the use by the Chinese government of online polls and its close analysis of hot topics and popular online comments. In recent years, ministries have been using the Internet to keep up with popular demands, anticipate complaints, and in general terms try to reduce the disconnect between officials and the lives and expectations of the "ordinary people" (*laobaixing*)[8]. Online monitoring and polling is launched and supervised at various levels, by both central and provincial administrations. In general terms, opinion trends emerging from online comments and polls seem to be increasingly taken into account in the domestic policy-making process.

In a country where street demonstrations and elections are not taking place, it appears that the Internet is one of the rare sources that the central government can rely upon

8 See for instance, "Public opinion sought on draft decree on social assistance", Xinhua, January 2nd, 2014, English version available here: http://news.xinhuanet.com/english/china/2014-01/02/c_133014355.htm

to keep up to date with the opinion trends of the domestic population, and hope to maintain some form of legitimacy by addressing the most popular issues. In fact, the "democracy of opinion" processes observed in the majority of Western countries exist in another form in China, in a different political context. A form of authoritarianism of opinion can be seen from the way the single-party is paying attention to opinion trends emerging on participative Internet platforms.

3.2. Latest adjustments under Xi Jinping

3.2.1. *Smart management of the Internet: a top priority under the new leadership*

Under the new Chinese leadership led by Xi Jinping, Internet management is more than ever mentioned as a top priority for the government. The leadership transition had been partly troubled by online debates and discussions on various scandals and news releases (Bo Xilai scandal, release on several Western media of the wealth of several top leaders and their family members, etc.), and the new team arrived to power fully conscious of the challenges that the development of social networks poses to the official aims of "social harmony" and political stability.

Once the 18th Party Congress was over and the new standing committee appointed, Beijing started to launch a stricter set of rules regarding social network use. In December 2012, it adopted a rule ushering in "a new era of cyberspace management", according to a journalist of the state-owned Xinhua press agency:[9] Internet users are accordingly required to use their real names when signing Web access agreements with service providers. In practice, implementation of this rule appeared difficult and

9 Xinhua News Agency, "New rules usher in new era of Internet management", by Wang Aihua, December 28th, 2012, http://news.xinhuanet.com/english/indepth/2012-12/28/c_132069951.htm

incomplete. Both Internet users and service providers were reluctant to adopt it for different reasons (barriers to freedom of expression[10], but also barriers to business developments, from the viewpoint of enterprises). However, it marked a reinforcement of Internet control under the new leadership. Indeed, the focus on Internet management was reinforced throughout 2013. In addition to the above mentioned rule, new rules against the spread of so-called rumors and personal attacks were issued[11] and several leading bloggers and social media commentators were punished.[12]

In the same line, official declarations on the topic suggests that the central government expects further reinforcement of Internet control in addition to the existing fast and comprehensive automated and human-led censorship mechanisms. Internet management is considered as a top "public security" priority, within the document "Decision on Major Issues Concerning Comprehensively Deepening Reforms", which list key general objectives and areas of reform adopted at the close of the Third Plenary Session of the 18th CPC Central Committee in mid-November 2013:

> *"Improving the public security system. (…) We will strengthen comprehensive measures for public security, introduce multi-tiered prevention and control system for public security, and strictly guard against and punish all sorts of unlawful and criminal activities in accordance with the law. Adhering to the principles of*

10 It raised debates and discussions among users. See for instance, "Internet ID policy triggers online discussion", Xinhua/China Daily, January 4th, 2013, http://www.chinadaily.com.cn/china/2013-01/04/content_16078594.htm.

11 In 2013, the Supreme People's Court and Supreme People's Procuratorate released a judicial opinion announcing that any online rumors which is "clicked and viewed more than 5,000 times, or reposted 500 times" would be viewed as "serious defamation" and could lead to jail sentences of up to three years.

12 Such as the closure in May 2013 of the accounts of Muron Xuexun, a famous author with more than 4 millions followers on his Weibo account.

> *active utilization, scientific development, law-based management and ensured safety, we will strengthen management of the Internet in accordance with the law, accelerate the improvement of leadership system for Internet management, and guarantee the country's Internet and information safety. We will establish the Council of State Security and improve the national security system and strategies to guarantee the country's national security."*[13]

The explanatory speech given by Xi Jinping related to these decisions is even more specific on the matter. Internet management appears as one of the 11 major issues underlined by the President (issue number 8):

> *"Eighth, concerning accelerating the perfection of leadership systems for Internet management. Network and information security involve national security and social stability, and this is a new comprehensive challenge that we face.*
>
> *From the point of view of practice, and in the face of the flying development of Internet technology and applications, clear malpractices exist in the current management system, which mainly are multi-headed management, overlapping of functions, lack of unity of powers and responsibility and low efficiency. At the same time, following the fact that the media nature of the Internet becomes ever stronger, online media management and sector management can by far not catch up with the developments and changes of the situation Especially in the face of micro blogs, WeChat and other such social media that have rapid dissemination, great influence, broad coverage and a strong capacity for social mobilization, as well as the*

13 Official, abridged English version of the full text of the document available at: "The Decision on Major Issues Concerning Comprehensively Deepening Reforms in brief", China Daily, November 16, 2013, http://www.china.org.cn/china/third_plenary_session/2013-11/16/content_30620736.htm.

> *rapid growth of instant telecommunication tool users, how to strengthen the construction of an online legal system and public opinion guidance, and ensuring the online information dissemination order, national security and social stability, have become current prominent issues put in front of us.*
>
> *The Plenum Resolution puts forward persisting in the principles of positive use, scientific development, management according to the law and guaranteeing security, expanding power to manage the network according to the law and perfecting leadership systems for Internet management. The objective is to integrate the functions of related organs, shape joint forces for Internet management from technology to content, from daily security to attacking crime, and guaranteeing the correct use and security of the network."*[14]

This official declaration appears in line with the previous one released under the Hu Jintao leadership. For instance, in the speech delivered by Hu, then outgoing *Party* chief, at the opening of the *18th Communist Party Congress* in November 2012, he mentioned, under a sub-part entitled "Enrich people's intellectual and cultural lives", the following:

> *"(…). We should improve the contents of online services and advocate healthy themes on the Internet. We should strengthen social management of the Internet and promote orderly network operation in*

14 "Explanation concerning the "CCP Central Committee Resolution Concerning Some Major Issues in Comprehensively Deepening Reform"", speech given by Xi Jinping at the 3rd Plenum on November 15th, 2013, which aims to provide a background to the resolution. Full, non-official English translation of the text available at: http://chinacopyrightandmedia.wordpress.com/2013/11/19/explanation-concerning-the-ccp-central-committee-resolution-concerning-some-major-issues-in-comprehensively-deepening-reform/; Full, official Chinese version of the speech (关于《中共中央关于全面深化改革若干重大问题的决定》的说明, 新华网北京11月15日) available at http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm.

> *accordance with laws and regulations. We should crack down on pornography and illegal publications and resist vulgar trends. (…).*"[15]

However, what is new with the explanatory speech given by Xi Jinping is that it explicitly mentions the social network that currently appears to cause a problem to the new leadership (the mobile messaging application WeChat).[16] This network is likely to be monitored to a larger extent under the current leadership. In general terms, Mobile apps will be monitored closely as the government is facing a new challenge in its Internet management strategy: the very fast-paced increase of China smart phone users, connected continuously to the Internet. The size of smart phone users increased sharply over the last two years, surpassing the number of users who use desktops in the middle of 2012.[17]

In addition, the latest official statements clearly underline the new leadership's willingness to reinforce the use of the Internet as a political communication tool, in a participative manner through various social networks and other online platforms. For instance, among the Decisions adopted at the close of the Third Plenary Session of the 18th CPC

15 Full text of Hu Jintao's report at 18th Party Congress, official English version: Xinhua, November 17th, 2012, http://news.xinhuanet.com/english/special/18cpcnc/2012-11/17/c_131981259.htm.

16 Also noticed by Paul Mozur, The Wall Street Journal/China Real Time blog, "China Wants to Control Internet Even More", Paul Mozur, November 15, 2013, http://blogs.wsj.com/chinarealtime/2013/11/15/china-wants-greater-internet-control-public-opinion-guidance/.

17 According to official figures: "By the end of December 2012, China has had 422 million mobile phone Internet users, 64.4 million more than that of the end of 2011. Among all the Internet users, those using mobile phones to access Internet increased from 69.3% at the end of 2011 to 74.5%", Statistical Report on Internet Development in China, China Internet Network Information Center (CNNIC), January 2013, http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf.

Central committee in mid-November 2013, was also mentioned the following:

> *"Bringing the people's congress system in line with the times.**(…)** We will increase the contacts between the Standing Committee of the NPC and the NPC deputies, and give full play to the role of deputies. Deputy liaison offices and Internet platforms will be established in people's congresses to increase deputies' contact with the people. We will improve the working mechanism of people's congresses, widen channels for the public to participate in legislative work in an orderly manner through discussion, hearing, assessment and publicizing draft laws; actively address social concerns through inquiry, investigation of specific problems, and putting on record for examination."*[18]

The use of public opinion is extremely strategic for the new leadership, who nowadays talk about "supervision through public opinions", for instance regarding its nationwide anticorruption campaign launched in 2013 and largely mentioned during the 3rd plenum:

> *"Be more innovative in creating mechanisms and institutions to combat corruption. (…). We will experiment with publicizing personal information of newly appointed officials. We will improve democratic and legal supervision as well as supervision through public opinions, and apply and regulate Internet supervision."*[19]

So far, the new leadership to some extent encouraged Internet users to expose graft and corruption among government officials. Online tracking and denunciations led

18 Official, abridged English version of the full text of the document: "The Decision on Major Issues Concerning Comprehensively Deepening Reforms in brief", China Daily, November 16, 2013, http://www.china.org.cn/china/third_plenary_session/2013-11/16/content_30620736.html.

19 *Ibid.*

to several high-ranking officials getting sacked in 2013. For instance, Chinese bloggers pointed to luxury watches on online photos of an official, which was later convicted of corruption and sentenced to prison.[20] This development echoed the official concept of "supervision by society over the Internet industry" which started to emerge in recent years[21]. But the Party also appears conscious that it represents a double-edge sword practice that can lead to excesses[22] and risky settling of scores among party cadres.

Another development indicating that Internet management is a top priority in the eyes of the new leadership is the creation of a new dedicated top-level institution. Indeed, a central leading small group – traditionally known in the PRC to support high-level decision making process – has been created in February 2014 to "lead and coordinate Internet security and informatization work among different sectors"[23]. The rank of this new group headed by Xi Jinping himself (one of three groups newly created and led by members of the Standing Committee of the Political Bureau of the CCP Central Committee. The other two include a state security committee and central leading team for comprehensively deepening

20 See for instance, "China's "Brother Watch" sentenced to 14 years in prison", The Telegraph, September 5th, 2013.http://www.telegraph.co.uk/news/worldnews/asia/china/10287972/Chinas-Brother-Watch-sentenced-to-14-years-in-prison.html.

21 For instance, Speaking at the 2012 China Internet Conference, Miao Wei, then minister of industry and information technology, said a comprehensive management system will be introduced to include government management, industrial self-regulation and supervision by society over the Internet industry. Xinhua News Agency, "China to tighten Internet management", September 11th, 2012, http://news.xinhuanet.com/english/china/2012-09/11/c_131843693.htm.

22 See for instance, "China fights 'harmful Internet activities'", The Diplomat, Shannon Tiezzi, December 19, 2013, http://thediplomat.com/2013/12/china-fights-harmful-internet-activities/.

23 Xinhua News Agency/People's Daily "China Eyes Internet Power", March 8th, 2014.http://english.peopledaily.com.cn/90785/8559640.html.

reform) underlines the degree of importance of Internet related issues under the new leadership.

3.2.2. *"Guiding public opinion"…*

The guidance of public opinion is a long term practice in the People's Republic of China, where traditional propaganda banners have always been widespread in public spaces since its creation in 1949. But such practice has taken new forms lately with the development of the Internet and social networks. In January 2014, senior official Liu Yunshan stressed increased capability in guiding public opinion and the creation of a "positive and upward" atmosphere on the Internet.[24] He also emphasized the leadership of the Party over the media, the correct guidance of public opinion, and the pooling of positive energy.[25] His speech also calls for a reinforcement of the power of institutions in charge of controlling media, including the Internet.[26] Most of all, Liu Qibao, head of the Publicity Department of the Central Committee, called for "greater efforts to guide public opinion on the Internet and strengthened guidance and management in the ideological sphere"[27].

This indicates that the central and local governments will probably continue to "guide public opinion" through

24 Xinhua News Agency, "Chinese official stresses increased capability in guiding public opinion", January 3rd 2014, http://news.xinhuanet.com/english/china/2014-01/03/c_125954678.htm.
25 *Ibid.*
26 "Publicity departments should become powerful in order to do a good job in publicity and ideological work 'under new situations'," said Liu, according to Xinhua News Agency, "Chinese official stresses increased capability in guiding public opinion", January 3rd 2014, http://news.xinhuanet.com/english/china/2014-01/03/c_125954678.htm.
27 According to Xinhua News Agency, "Chinese official stresses increased capability in guiding public opinion", January 3rd 2014, http://news.xinhuanet.com/english/china/2014-01/03/c_125954678.htm.

traditional means (spreading of red propaganda/banners online, hiring of online commentators supporting the Party line, etc.), as well as through new means. It remains unclear what this means will be at the moment. But recent declarations indicate future attempts to develop new, fully Party-affiliated social networks and mobile apps.[28] It is likely that the new strategy to "guide public opinion" will cover a wide range of content, beyond Chinese language content and sites, as the new leadership is more than the previous one pointed at the "hostile Western forces" (from NGOs to media) that are trying to "demonize" and "destabilize" China,[29] and investing in a wide public diplomacy strategy through party-affiliated media in foreign languages.

3.2.3. *…while seizing economic opportunities*

The Chinese authorities are juggling between their two top aims: domestic economic development and political stability. The Internet represents both new sources of economic growth and political instability in the country.

---

28 "The Chinese media, under the leadership of the CPC, need to quicken their expansion into digital and new media and develop Internet and mobile offerings. That will allow them to maintain their ability to direct public opinion", said Li Congjun, President of Xinhua News Agency, in an editorial published in People's Daily (Party affialiated newspaper) in September 2013. Li also added "If we cannot effectively rule new media, the ground will be taken by others, which will pose challenges to our dominant role in leading public opinion" – quoted in english by China Economic, "Xinhua chief: Chinese media must lead public opinion and combat distorted views", September 5th, 2013, http://en.ce.cn/subject/exclusive/201309/05/t20130905_1327957.shtml

29 For instance, Li Congjun, President of Xinhua News Agency, said in the same September 2013 editorial that "some Western media outlets are trying to demonize China and sow national disintegration as they hate seeing the country prosper". China Economic, "Xinhua chief : Chinese media must lead public opinion and combat distorted views", September 5th, 2013, http://en.ce.cn/subject/exclusive/201309/05/t20130905_1327957.shtml.

In recent years, the Internet in China – from online applications to shopping websites such as Taobao[30] – not only became a major challenge to socio-political stability but also a major source of domestic economic growth. In this context, positive or negative consequences on the economy are carefully taken into consideration by the government before it takes decisions regarding the management of the Internet. The necessity of NTIC development to support the country's economic growth and modernization is the main reason the government has been tolerating to a certain extent the fast-paced development of the Internet and social networks on its territory, although it has represented significant political challenges since its emergence.

The current leadership is very conscious that the international attractiveness of Chinese e-companies remains limited and that their international development strategy remains incomplete.[31] It is therefore nowadays trying to push for the development of new online industries, such as Internet finance or security.[32] The Internet is now officially identified as a key sector to support China's economic growth. Internet security in particular appears as an industry which can generate growth while at the same time provide the government with new tools to more easily manage the Internet according to its will. It is certainly

30 For instance, e-commerce generated in 2012 a total revenue between 190-210 US$ billion, almost as much as in the US (220 and 230 US$ billion). And McKinsey, the consultancy, reckons in its report "China e-tail Revolution" that by 2020, China will become the top 1 e-commerce market. Le Monde, "La Toile où le prince est un Français", Brice Pedroletti, March 23, 2013.

31 "Although the country has nurtured IT companies with global reach, such as Tencent and Alibaba, an overall improvement across the sector is still badly needed.", underlines official media. Xinhua News Agency/People's Daily "China Eyes Internet Power", March 8th, 2014. http://english.peopledaily.com.cn/90785/8559640.html

32 "China Eyes Internet Power", Xinhua News Agency/People's Daily, March 8th, 2014.

because it is compatible with the government's top two aims (economic development and political stability), and not only because of the recent PRISM scandal and tit-for-tat exchanges opposing the US and China, that Beijing is now identifying it as a key strategic sector to focus on and invest in.

3.3. Bibliography

[BEN 13] BENNEY Jonathan, KING Gary YANG Guobin, The Great Firewall of China, China Policy Institute Blog, November 3, 2013, http://blogs.nottingham.ac.uk/chinapolicyinstitute/2013/11/03/the-great-fearwall-of-china/.

[CHI 13] CHINA DAILY, The Decision on Major Issues Concerning Comprehensively Deepening Reforms in brief, November 16, 2013, http://www.china.org.cn/china/third_plenary_session/2013-11/16/content_30620736.htm.

[CHI 13] China Internet Network Information Center (CNNIC) Statistical Report on Internet Development in China, January 2013, http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf.

[KIN 13] KING Gary, PAN JENNIFER, and ROBERTS Margaret E. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review*, 107, (2 (May): 1-18.

[MOZ 13] MOZUR Paul, "China Wants to Control Internet Even More", *The Wall Street Journal/China Real Time blog*, November 15, 2013.

[SCH 13] SCHNEIDER Florian, The Mass-Media logic behind China's Internet Controls, November 11, 2013, http://www.politicseastasia.com/uncategorized/mass-media-logic-behind-chinas-internet-controls/.

[WAN 12] WANG Aihua, New rules usher in new era of Internet management, Xinhua News Agency, December 28th, 2012, http://news.xinhuanet.com/english/indepth/2012-12/28/c_132069951.htm.

[XIN 13a] Xinhua News Agency/China Daily, Internet ID policy triggers online discussion, January 4th, 2013, http://www.chinadaily.com.cn/china/2013-01/04/content_16078594.htm.

[XIN 13b] Xinhua News Agency/China Daily, Expert defends China's Internet management, February 4th, 2013, http://www.chinadaily.com.cn/china/2013-02/04/content_16198768.htm.

[XIN 13c] Xinhua News Agency, (习近平：关于《中共中央关于全面深化改革若干重大问题的决定》的说明, 新华网北京11月15日) http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm. [Explanation concerning the CCP Central Committee Resolution Concerning Some Major Issues in Comprehensively Deepening Reform, speech given by Xi Jinping at the 3rd Plenum on November 15th, 2013.]

[XIN 14a] Xinhua News Agency, Public opinion sought on draft decree on social assistance, January 2nd, 2014, http://news.xinhuanet.com/english/china/2014-01/02/c_133014355.htm

[XIN 14b] Xinhua News Agency, Chinese official stresses increased capability in guiding public opinion, January 3rd 2014, http://news.xinhuanet.com/english/china/2014-01/03/c_125954678.htm.

[XIN 14c] Xinhua News Agency/People's Daily, March 8th, 2014. China Eyes Internet Power, http://english.peopledaily.com.cn/90785/8559640.html.

[YAN 11] YANG Guobin, China's Gradual Revolution, Opinion pages, The New York Times, March 13, 2011, http://www.nytimes.com/2011/03/14/opinion/14Yang.html?_r=0.

[YAN 12] YANG Guobin, "A Chinese Internet? History, Practice, and Globalization", *Chinese Journal of Communication*, Special issue on "Chinese Media and Globalization", vol. 5, no. 1, pp. 49–54, 2012.

[ZHI 12] ZHI Chen, China to tighten Internet management, XINHUA News Agency, September 11th, 2012, http://news.xinhuanet.com/english/china/2012-09/11/c_131843693.htm.

4

India's Cybersecurity – The Landscape

Cyberspace presents all the conditions for a perfect storm; it is open, global but insecure. Usage is at an all time high with users ranging from individuals to corporations to governments, all using the same pipes for the transmission of some or all of their data and communications, and equally subject to the inherent vulnerabilities in cyberspace. Governance is at a nascent stage, with negotiations in different fora proceeding at an excruciatingly slow pace as differences arising from a number of different perspectives have to be resolved. At the same time, the number of attacks with politico-military objectives is on the rise, leading to a steady militarization of cyberspace with many countries forming Cyber Commands to undertake offensive actions in and through cyberspace.

While India was among the first countries to have an Information Technology Act, and to set up a Computer Emergency Response team (CERT), and even to locate responsibility for cybersecurity within the National Security

---

Chapter written by Cherian SAMUEL. The views expressed are personal and do not reflect the views of the IDSA or the Government of India.

Council, it has subsequently lagged behind other countries in responding to cybersecurity threats.

India has been at the receiving end of various forms of cyber threats; from attacks on critical infrastructure, to cybercrime, to the latest manifestation of the misuse of social media. Responses at the official level have been marked by several mis-steps. Till recently, there was an inadequate appreciation of the cybersecurity threats at the official level, though that is no longer the case. However, the responses to the threats, as well as the effort to shape cyberspace policy at the domestic level, and the contribution to discussions at the international level, still leave much to be desired.

4.1. A snapshot of Asian cyberspace

According to the latest statistics, 44 percent of all Internet users, amounting to nearly a billion people, are in Asia. At the same time, Internet penetration in Asia was at 26.2 percent compared to the global average of 32.7 percent[1]. Within Asia, China stood first with an online population of 513 million, followed by India with 121 million and Japan with 101 million. The developed regions of North America, Europe and Oceania were nearly saturated with a penetration rate of 70%. Online population rates are increasingly translating into offline clout, with a resultant say in everything from the development of standards and technologies, to the success or failure of Ecommerce undertakings.

Other characteristics of Asian cyberspace include the following:

1 Internet World Stats, http://www.internetworldstats.com/stats3.htm.

– the top 5 countries in terms of average broadband speeds are in Asia, led by Hong Kong. According to the latest Akamai State of the Internet Report, Hong Kong secured the top spot with an average peak connection speed of 49.2 Mbps; South Korea had 47.8 Mbps and Japan claimed third place with 39.5 Mbps[2].

– China is the hardware factory of the world with economies of scale and government policies ensuring that "Made-in-China" products beat their competitors hollow. This has strategic implications especially in the cyber arena because of fears that such products, especially in sensitive areas such as networking might be compromised.

– India is a leader in IT services and software development, while other countries like the Philippines and Malaysia are also seeking to increase their global share in these sectors.

– According to a McKinsey report, cyberspace contributed 3.5 percent to the economies of 13 countries surveyed in 2011, including India and China.[3] As Internet penetration increases, this would be expected to go up proportionately.

– Many countries in Asia are also heavy users of e-governance, with the government of India alone expected to spend about $33 billion on its flagship Unique Identification program by the time it is completed.

– Asia is also home to some of the larger cyberpowers. Cyberpower is, at present, a generic term referring to actual or potential cyber capabilities based on various indices.

---

2 Akamai State of the Internet. 1 Aug. 2012. Akamai. Accessed on 21 Sept. 2012 http://www.akamai.com/stateoftheinternet/>.

3 Manyika, James *et al.*, (ed.), *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*. Rep. McKinsey Global Institute, May 2011. Web. Accessed on 15 Sept. 2012. http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters.

These include population and the state of technological development.

While threats have existed right from the early days of cyberspace, the sporadic patterns of such attacks and their targets suggested them to be largely the handiwork of hackers and low level criminal elements. The major delivery vehicles were spam mails which contained viruses and malware. The problem was manageable and up-to-date antivirus programs and firewalls were deemed to be sufficient to keep such risks at bay. Subsequently, new forms of malware such as Worms and Trojans, which exploited the vulnerabilities in buggy software, also began to make their appearance. Phishing and denial of service (DoS) attacks also entered the lexicon. All these threats[4] took advantage of existing vulnerabilities[5], whether it be in software, networks or security architecture.

While governments and government agencies, from the military to the intelligence community, have always had the ability to carry out disruptive activities in cyberspace, the absence of such activities, other than the attacks out of Russia on Estonian and Georgia in 2007 were attributed to forbearance, keeping in mind the cascading effects of such

4 A threat was defined by the Computer Emergency Response Team (CERT) in 1993 as "Any circumstances or event that has the potential to cause harm to a system or network. That means, that even the existence of a(n unknown) vulnerability implies a threat by definition".

5 Vulnerabilities are defined as a) a feature or bug in a system or program which enables an attacker to bypass security measures; b) an aspect of a system or network that leaves it open to attack, and c) the absence or weakness of a risk-reducing safeguard which had the potential to allow a threat to occur with greater frequency, greater impact or both. Anil Sagar, *An Overview to Information Security and Security Initiatives in India*, Powerpoint Presentation, 18 January 2008. Available online at *www.elitex.in/paper2008/anilsagar.ppt.*

actions.[6] But as larger numbers of actors have entered the domain, attacks are becoming more and more disruptive and even destructive in nature. Many perceived red lines have been crossed; it was believed that attacks on critical infrastructure would only take place in conjunction with a kinetic war, that countries would disconnect from the global information grid only with peril to their economies and societies, and that countries with roughly symmetrical capabilities and capacities for cyberwarfare would refrain from attacking each other, but all these have already taken place.

The attractiveness of using cyber as a means of bloodless attacks has led to powers both within and outside the region using these means to achieve politico-military objectives, which is leading to an ongoing cycle of retaliation and counter-retaliation. Thus, a combination of existing fault lines and the easy access to cyberspace as a new means of perpetrating conflict is one of the reasons leading to cyberconflict.

Faced with this developing reality, countries of the Asian region have been at the forefront of reshaping cyberspace according to their perceptions and in some cases, strategic priorities. While a country like North Korea has completely cut itself off from cyberspace, Iran is also on the way to having a separate countrywide intranet which is separate from the Internet. While Saudi Arabia has only one gateway into the country where all data is filtered, China has the great firewall which also performs a similar function. Such

6 In 2003, the US intelligence agencies drew up plans for a cyber-attack designed to freeze Iraq's financial system but the Bush administration, concerned about the possibility of a ripple effect leading to worldwide financial havoc, refused to give the go-ahead. *The New York Times*, Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, 1 August 2009. Available online at http://www.nytimes.com/2009/08/02/us/politics/02 cyber.html.

restrictions serve a dual purpose of being virtual borders while also allowing for content monitoring under the guise of national security.

While Indian policy makers are aware of the issues and have responded with policies, legislation, organizations and mechanisms that have been put in place over a period of time, the assessment from security analysts is that this is still inadequate to meet the challenges. This is because, as in the real world, India is in a rough cyber neighborhood. It has to balance its commitments to an open, secure and global cyberspace and at the same time surmount the threats thrown up by the vulnerabilities in and through cyberspace to its national security.

4.1.1. *Aspects of cyberconflict in Asia*

Cyberspace has become a natural adjunct to many of the ongoing conflicts in Asia. The severity and escalation of cyberconflicts in this region is directly proportional to the hostilities offline. Current cyber flashpoints can be located throughout the length and breadth of Asia, ranging from attacks in West Asia, East Asia and, to a lesser extent South Asia. It may be seen that the attacks are carried out through the available infrastructure without respect to geographic boundaries.

4.1.2. *West Asia*

A combination of the volatility of West Asia and the involvement of technologically advanced powers from both within and without the region in the hostilities there have made this region a frontline of cyberconflict, as well as an indicator of emerging trends in cyberconflict.

The Stuxnet malware in 2010 was the first "cyber-weapon" and its success in disabling Iranian centrifuges

brought the issue of cybersecurity to center stage. Stuxnet was directed against the Iranian nuclear program, and suspicions of US and Israeli involvement were confirmed by subsequent reports. These suspicions arose in the first place because of the sophistication of the malware, which, experts declared, could only be engineered through the resources available to a nation state. It was the first large-scale attack on critical infrastructure that ran on SCADA systems.[7] While there have always been concerns about supply chain integrity, Stuxnet showed how even normal vulnerabilities can be utilized in cyber-attacks. The national origin of companies assumes even more significance in this regard.

Offshoots of Stuxnet have been discovered with regularity since then: the Duqu worm was discovered in September 2011, followed in quick succession by the Mahdi, Gauss and Flame malware. While Flame, Duqu and Gauss were said to share similar digital DNA with Stuxnet, being spread predominantly via USB sticks, their primary purpose seemed to be espionage, with their targets ranging from banking, governmental to energy networks. Flame, in particular, was noted for its modular nature, and its size, averaging 20 MB. Its capabilities ranged from recording Skype conversations and downloading information from smart phones to more mundane activities such as recording audio, screenshots, keystroke and network traffic recording. The Mahdi Trojan seemed to have different godfathers and was spread via phishing emails even though its purpose was also apparently espionage. Infections were reported from Iran, Israel, Afghanistan, the United Arab Emirates, Saudi Arabia, Syria, Lebanon and Egypt.[8]

---

7 According to are estimate, it took the equivalent of 6 man years and around 1.5 million dollars to develop.

8 *Guardian.* Cyberwar on Iran more widespread than first thought, say researchers. (2012, September 21). Retrieved from http://www.guardian.co.uk/technology/2012/sep/21/ cyberwar-iran-more-sophisticated.

In April 2012, there were reports of a new virus, Wiper, which was much more malicious, and wiped off the data on all computers that it infected. This virus largely affected networks in Iran. Four months later, the Shamoon virus is reported to have wiped off the data from 30,000 computers of the Saudi Arabian State oil company, Aramco, followed a week later by a similar episode on the networks of the second largest LNG company in the world, Ras Gas of Qatar.

In what has become the norm for such cyber-attacks, despite intense investigations by anti-virus companies, the origins of the malware have remained largely in the realm of speculation and inference. While ownership of the Stuxnet (and by inference, its cousins Duqu, Flame and Gauss) malware was claimed by the Obama Administration for electoral purposes, the Shamoon virus was speculated to be a reverse-engineered version of the Wiper virus unleashed by hackers loyal to the Iranian regime.[9] Each successive attack represents a relentless and rapid escalation in capabilities and intent on the part of the perpetrators. The increasing use of drones in West Asian conflicts and repeated occurrences of hacking into drones has raised the possibility that such hijacked drones could be turned against their controllers.[10]

9 However, as David Betz notes, anonymity is as much a problem for the aggressor as it is for the target. Clues have been left in malware software both to misguide and to claim ownership. Betz, D. (2012, June). *Cyberpower and International Security* [PDF]. Retrieved from http://www.fpri.org/enotes/2012/201206.betz.cyberpower-international-security.pdf.

10 *Washington Post*. "Remote U.S. base at core of secret operations." October 26, 2012. Accessed October 30, 2012. http:// www.washingtonpost.com/world/national-security/ remote-us-base-at-core-of-secret-operations/2012/10/25/ a26a9392-197a-11e2-bd10-5ff056538b7c_ story.html.

Iran has shown how rapidly cyber capabilities can be acquired; from having virtually no capabilities before 2009, it has now acquired significant expertise, and is using them. This is what the United States is finding out to its cost as US banks are subject to a sustained volley of DDOS attacks by a hacker group calling itself Izz ad-Din al-Qassam Cyber Fighters, but believed to be Iran retaliating for cyber-attacks on its infrastructure.[11] While the United States has begun to raise cybersecurity related issues with China in its strategic dialogues, no such scope exists in the case of Iran, which like the United States, sees advantages in plausible deniablity accorded by cyberspace. In other words, this is the online version of a low-intensity conflict, continuing endlessly till one or the other side ratchets up through retaliation. The end result might very well be different if such a scenario is played out elsewhere since the absence of collateral damage in this case is largely afforded by the technical capabilities of the US.

According to James Lewis, Iran's expanding cyber capabilities have the potential to change the balance of power.[12] As a guarantor of security in the Persian region, the United States has provided assistance to its allies in the area but the majority of countries are making use of private contractors.[13]

11 New York Times, *Bank Hacking Was the Work of Iranians, Officials Say,* 8 January 2013. Available online at http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

12 Lewis, James A. *Cybersecurity and Stability in the Gulf*. Issue brief. 6 January 2014. CSIS. Available online at http://csis.org/publication/cybersecurity-and-stability-gulf. Accessed on 6 February 2014, p. 1.

13 Ibid. p. 4.

4.1.3. *East Asia*

Hostilities between countries in East Asia are also mirrored in cyberspace and China is a common factor in many of these conflicts. There have been DDOS attacks emanating from China into the Philippines, Vietnam and Japan, and vice versa. The dispute over Scarborough Shoal/Huangyan Island saw cyber-attacks between China and the Phillipines in April/May followed by a similar showdown between Chinese and Vietnamese hackers in May 2012 following an incident, and attacks by Chinese hackers on Japanese websites following the territorial dispute over the Diaoyu/Senkaku Islands in September 2012.[14]

Among the various protagonists in East Asia, North Korea has carried out an aggressive campaign against South Korea using every weapon in its arsenal and inflicting some real damage in the process. South Korea presents an easy target, being one of the most wired countries in the world, while North Korea does not even present itself as a target, having no networks worth speaking of. While not much information is available about the size of North Korea's cyber corps, South Korean estimates are that it has doubled in the last few years and now numbers around 3,000.[15]

China ranks far ahead of the other powers in Asia in terms of both capabilities and potential, according to Western and some Indian analysts. According to Western reports, the PLA has integrated cyberwarfare units since 2003 and has built up a huge cyber military edifice. The Third Department and Fourth Departments of the PLA,

14 *Japan Times* (Tokyo). "Japanese websites come under attack as Senkaku squabble continues". September 20, 2012. Accessed September 25, 2012. http://www.japantimes.co.jp/text/nn20120920b7.html.

15 N. Korea commands 3,000-strong cyber warfare unit: defector. (2011, June 1). Yonhap. Retrieved from http://english.yonhapnews.co.kr/northkorea/2011/06/01/46/0401000000AEN20110601004200315F.HTML.

responsible for military intelligence, have been described in reports as among the most powerful bureaucracies in not just the military but in China today with their access to every bit of information that criss crosses China.[16]

Other countries of the region are far behind the Chinese in incorporating cyberwarfare into general war fighting doctrines and building up capabilities. South Korea published a national cybersecurity strategy where it declared cyberspace to be an operational domain that needed a state level defense system. The National Intelligence Center was tasked with coordinating cybersecurity along with the Korea Communications Commission (KCC). The KCC has focused on a defensive role, detecting, preventing and "responding to cyber assaults".[17] As with other US allies in the region, South Korea also places a lot of emphasis on extending its relationship to cover cyberspace.

In the case of Japan, in its Annual White Paper, the Japanese Ministry of Defense listed "responding to cyber-attacks" as one of its priority areas. The self defense force (SDF) was tasked with defending not only its own networks but also with "accumulating advanced expertise and skills needed to tackle cyber-attacks" so as to contribute to the government-wide response to cyber-attacks.[18] In addition to the cyber vandalism, intellectual property from Japanese companies has also been the target of hackers with

16 Stokes, M., and Jenny Lin. *The Chinese People' S Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute, 2011.

17 "S. Korea charts out national cybersecurity strategy." Yonhap news Agency. Last modified August 8, 2011. Accessed October 30, 2012. http://english.yonhapnews.co.kr/techscience/2011/08/08/45/ 0601000000 AEN20110808006500320F.HTML.

18 *Annual White paper 2012*. Report. Tokyo, Japan: Ministry of Defense, 2012. Accessed September 26, 2012. http://www.mod.go.jp/e/publ/w_paper/ 2012.html.

the notable incident being the August 2011 hacking of Mitsubushi Heavy Industries as well as other technology firms.[19] In the same month, 480 members of the Japanese Diet had their email accounts compromised and their machines hijacked with the hijacked machines apparently communicated with a server in China.[20]

In September 2012, the Japanese Ministry of Defense announced that it would act on the recommendations of a panel constituted to examine threats in cyberspace and would constitute a 100-strong cyber unit with a budget of ¥21.2 billion (US$270 million).[21] The panel made a number of conceptual definitions, calling cyberspace a domain like air, sea, land and space. It was an essential infrastructure for the SDF to carry out their activities, and it was therefore, their responsibility to secure it. They would have to co-operate with a number of partners both domestically and internationally, and these partners could also be in the private sector.[22] Cyber-attacks would be considered on a

19 BBC Online. *Japan defence firm Mitsubishi Heavy in cyber-attack*. BBC. Last modified September 20, 2011. Accessed September 25, 2012. http://www.bbc.co.uk/news/world-asia-pacific-14982906.

20 "Upper House computers also hacked." Asahi Shimbun. Last modified November 3, 2011. Accessed September 25, 2012. http://ajw.asahi.com/article/behind_news/social_affairs/AJ2011110316472.

21 "Japanese defense panel: Cyber-attacks can be basis for military self defense." Computerworld. Last modified September 9, 2012. Accessed September 26, 2012. http://news.idg.no/cw/art.cfm?id=409AA657-DC59-0780-FF139675AC1AAE62. This is out of a defense budget of ¥4.7 trillion.

22 Ministry of Defense Panel on Cybersecurity. *Toward Stable and Effective Use of Cyberspace*. Tokyo, Japan: n.p., 2012. Accessed September 26, 2012. http://www.mod.go.jp/e/d_act/others/pdf/ stable_and_effective_use_cyberspace.pdf.

case-by-case basis, but if carried out as part of a military attack, it would respond in self-defense. [23]

Japan and the United States agreed in 2013 to increase "cyberdefense cooperation with the improvement of individual cyber capabilities and interoperability between the [Japan] Self-Defense forces and U.S. forces, which will also contribute to whole-of-government cybersecurity efforts"[24]. Taking a leaf out of the US playbook, Japan has also begun to use private contractors to develop cyberweapons.[25]

While most of the US allies are looking towards close cooperation with the United States, it has entered into a cyberwarfare cooperation program only with Australia, the only one outside of its program with NATO.[26] In October 2013, the two countries announced that they were setting up a joint Cyberdefense Policy Working Group to foster "increased cyberdefense cooperation with the improvement of individual cyber capabilities and interoperability between the [Japan] Self-Defense forces and U.S. forces, which will

23 Alabaster, Jay. "Japanese defense panel: cyber-attacks can be basis for military self defense." CIO. 07 Sept. 2012. Accessed on 23 March2013 . Available online at http://www.cio.com/article/715628/Japanese_Defense_Panel_Cyber_Attacks_Can_Be_Basis_for_Military_Self_Defense?

24 "Joint Statement of the Security Consultative Committee: Toward a More Robust Alliance and Greater Shared Responsibilities." *U.S. Department of State*., 03 October 2013. Accessed on 22 November 2013. Availabe online at http://www.state.gov/r/pa/prs/ps/2013/10/215070.htm.

25 "Japan Developing Cyber Weapon: Report." *The Australian* 2 Jan. 20122 January 2012. Accessed on 5 September 2013. Available online at www.theaustralian.com.au/technology/japan-developing-cyber-weapon-report/story-e6frgakx-1226234630603.

26 Baldor, Lolita. "Cyber cooperation added to US-Australia treaty." Businessweek, September 15, 2012. Accessed September 27, 2012. http://www.businessweek.com/ap/financialnews/D9POVN5G0.htm.

also contribute to whole-of-government cybersecurity efforts".[27]

4.2. The Indian cyber landscape

Many commentaries refer to India as a cyberpower,[28] something that might appear to be at odds with the reports regarding the vulnerabilities in India's cybersecurity that appear in the newspapers day after day. The Indian government itself estimates that there are only 556 cybersecurity experts in the country.[29]

Relatively low levels of computer security largely due to pirated software and the presence of patriotic hackers in the countries of the region have made the region a hotbed of low level hacking and website defacement. The so-called "cyberwars" that break out every now and then are a numbers game, and a hidden hand of the intelligence agencies can also be vaguely discerned. This is also probably why such attacks have not crossed any red lines, despite threats to bring down the financial systems and so on. The near equivalence of hackers in the countries of South Asia would point to a low level form of deterrence in existence. Nearly all upswings in defacements and hacking, which

27 "U.S.-Japan Set Road Map for Next 20 Years Amid Asian Threats." *Bloomberg.com*. Bloomberg, 03 October 2013. Accessed on 08 Jan 2014. Available on line at <http://www.bloomberg.com/news/2013-10-03/u-s-japan-to-expand-military-ties-for-first-time-in-16-years.html>.

28 For instance, see Interview with John Mroz, President, East-West Institute, *India: An Emerging Cyber power*. East West Institute, 24 September 2012. Available online at http://www.ewi.info/idea/india-emerging-cyber-power Accessed on 18 December 2012.

29 "An IT superpower, India has just 556 cybersecurity experts", *The Hindu* 19 June 2013. Available online at http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece Accessed on 20 June 2013.

normally follow a tit-for-tat pattern, have ended in truces being called by the hackers on various sides. Though these defacements are not more than the equivalent of digital graffiti, they show that more grievous damage could be easily inflicted.

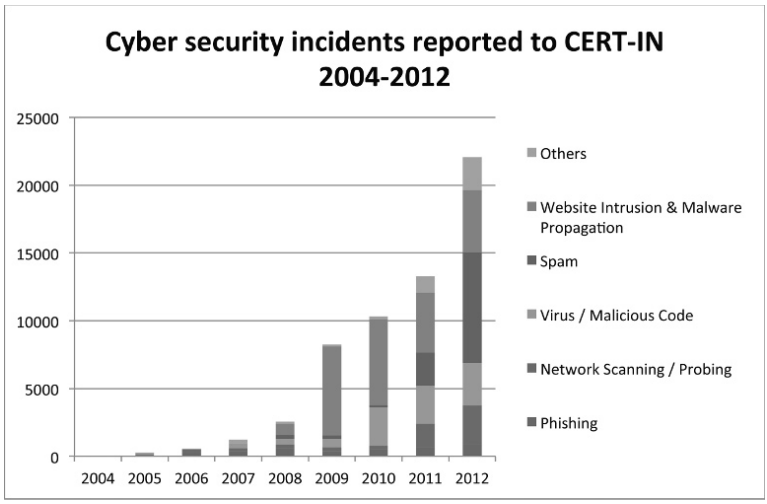


Figure 4.1. *Cybersecurity incidents reported to CERT-IN 2004-2012.*

While these occurrences grab the newspaper headlines, the more serious threats are elsewhere. Cyber-espionage and threats to critical information infrastructure are a clear and present, but invisible threat to national security. In the case of the former, given India's rising power status, sensitive networks and systems are subject to constant attempts at penetration. While some of these intrusions have been discovered by domestic agencies, many others have been discovered by external agencies, pointing to the long distance to be covered in securing Indian networks. With regard to the latter, critical information infrastructure protection is complicated by the fact that much of the infrastructure rests in private hands. This creates problems, not only in

co-ordinating cyber-security efforts but also for gauging the extent of the problem, since private companies are reluctant to acknowledge that they have been attacked and more often than not do not report such attacks.[30] A second order of threats emanates from the global supply chain in IT products that has been created, which creates ample opportunities for backdoors and vulnerabilities to be inserted into hardware, and increasingly, software.

There is also the overt militarization of cyberspace to be taken into account as more and more countries set up Cyber Commands. There has been no official role for the military in cybersecurity, other than that of protecting its own networks that have been reportedly penetrated on and off.[31] This, despite the Minister of Defence referring to cyber threats as a major threat to the nation in virtually every speech made to the apex military gathering, the Combined Commanders Conference over the past three years.[32] With the cyber arena now recognised as a new domain of war, setting up a force competent to achieve the dual objectives of defending the country from cyber-attacks in war and securing the military's network operations in peace is one that requires considerable thought.

30 News of most attacks and incidents of cyber-espionage, whether it be on Reliance, ONGC or ITC have invariably been reported by third parties. The companies concerned have not confirmed such attacks, and in some cases have denied these attacks ever occurred.

31 That has not stopped the Corps of Signals from describing itself as "the lead agency and nodal center for information and cybersecurity both within the Defence Services and at the National level" on the Indian Army's website. See online at http://indianarmy.nic.in/Default3.aspx?MenuId=Qd7lMkEdWdEACCESSED ON?

32 "Antony Asks Army to Build Cybersecurity Capabilities." *The New Indian Express*. 22 Apr. 2014. Accessed on 13 May 2014. Available online at http://www.newindianexpress.com/nation/Antony-Asks-Army-to-Build-Cyber-Security-Capabilities/2014/04/22/article2182471.ece.

4.3. The China challenge: a case study

While a combination of these threats could be followed through by any of the countries having advanced cyber capabilities, China is particularly unique in having the means and the motivation, as well as the opportunity, to borrow a formulation from criminal law. China and India have a history of hostilities, especially regarding contested borders, which continues to this day. At the same time, China is among the largest producers and providers of both consumer as well as capital goods in the information technology and other infrastructure spaces.

Reports of Chinese infiltration of sensitive networks is nothing new; in 2007, for instance, US officials were reported as saying that Chinese attacks against the Department of Defense (DoD) had reached the level of a "campaign-style, force-on-force engagement" with actions running the "gamut of technology theft, intelligence gathering, exfiltration, research on DOD operations and the creation of dormant presences in DOD networks for future action."[33] In that same year, and subsequently, the governments of the United Kingdom[34],

33 Federal Computer Weekly, *Cyber officials: Chinese hackers attack "anything and everything"*, 13 February 2007. Available online at http://www.fcw.com/online/news/97658-1.html#.

34 The *Times* reported that the Director General of MI5 had sent a letter to 300 chief executives and security chiefs highlighting "concerns about the possible damage to UK business resulting from electronic attack sponsored by Chinese state organizations, and the fact that the attacks are designed to defeat best-practice IT security systems." The Times, *Secrets of Shell and Rolls-Royce come under attack from China's spies*, 3 December 2007. Also see *China 'top list' of cyber-hackers seeking UK government secrets*, Times of London, 6 September 2007. Available online at http://www.timesonline.co.uk/tol/news/world/asia/article2393979.ece.

France[35], Belgium,[36] Germany[37] and India[38] also publicly stated that their systems and networks had been infiltrated and attacked by entities that had been traced back to China.

The first known cases of cyber-espionage were targeted at Tibetan organizations based in India. The organized nature of this infiltration was brought to light by a number of reports, beginning with the Shadows in the Cloud Report in 2010, followed by Operation Shady Rat in 2011 and Operation Red October in 2013. While the needle of suspicion points to foreign intelligence agencies, and many of the attacks have been traced to China, conclusive proof is difficult to come by because of the ease with which such attacks can be spoofed in cyberspace. There had been earlier suspicions that probing and espionage efforts might also be coming from a third country and spoofed to make it seem that it was emanating from China.[39]

There is a considerable amount of Western literature pointing to the fact that the cyber-espionage activities are of a piece with Chinese formulations on assymetric warfare.

---

35 AFP, *La France victime de cyber-attaques avec "passage" par la Chine,* 8 September 2007. Available online at http://afp.google.com/article/ALeqM5i6dSqt39zfQcKG-I-HZUTRaN3Zvw.

36 vnunet.com, *Belgium accuses China of cyber-crimes*, Available online at http://in.ibtimes.com/articles/20080520/china-hacking-computer-hacker.htm

37 London Times, *China accused of hacking into heart of Merkel administration*, 27 August 2007. Available online at http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece

38 DNA India, *Chinese hackers penetrate crucial MEA network,* 10 April 2008. Available online at http://www.dnaindia.com/report.asp?NewsID=1159279 Also see DNA India, *Cyber-attack on 10 govt websites,* 7 June 2008. Available online at http://www.dnaindia.com/report.asp?newsid=1169339

39 Datta, Saikat. *""DNA' "Investigation: PMO Fights Largest Cyber-attack."* *DNA* [Mumbai] 22 Aug. 2011: Accessed on 22 March. 2012. Available online at http://www.dnaindia.com/india/report-dna-investigation-pmo-fights-largest-cyber-attack-1578348.

The earliest elaboration of the Chinese perspective was in the appropriately named treatise on warfare entitled "Unrestricted Warfare" by two colonels of the Peoples Liberation Army in 1999. The authors observed:

> Does a single "hacker" attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle?...Obviously, proceeding with the traditional definition of war in mind, there is no longer any way to answer the above questions. When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare.
>
> If this name becomes established, this kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten.

It would seem that the rules of war have indeed been re-written with Peoples Liberation Army units actively involved in cyber-espionage activities not just in wartime, but in peacetime as well.

According to Dean Cheng, PLA thinking on future wars is marked by the 3 nons – non-contact, non-linear and non-symmetric.[40] Non-contact would include computer network

40 Dean Cheng, *The Chinese People's Liberation Army and Special Operations,* Special Warfare, vol.25, issue 3, July-September 2012. Available online at http://www.soc.mil/swcs/SWmag/archive/SW2503/SW2503TheChinesePeoplesLiberationArmy.html.

operations "that will effectively nullify an opponent's forces without having to directly confront or engage them".[41] Following on from that, non-linear and non-symmetric war would take place in many dimensions, both physical and temporal, and not necessarily within a set battlefield or theatre.

Non-symmetric envelopes the previously mentioned strategic objectives of securing advantage over other countries even during peacetime through use of its cyber prowess in every spectrum from political, economic, scientific, and diplomatic and cultural arenas. To the PLA, non-symmetric war justifies the use of methods such as hacking and expropriating intellectual property 1) as a tool for getting access to and parity with the advanced technologies of the West and 2) as part of psychological warfare (through visibly penetrating networks in other countries and raising the spectre of cyber instability).

All of the above has to be juxtaposed against the fact that China is a major supplier to India of infrastructure equipment in areas from power to transport, and crucially to telecom hardware. India bought over $12 billion worth of mobiles, and $8 billion worth of computers and peripherals, making up nearly 23% of total imports.[42]

Chinese companies are able to beat other companies, both Indian and foreign, by bidding at the lowest possible prices and providing quality products. Indian intelligence agencies have noted similar tactics in neighboring countries as well.[43]

---

41 Ibid.

42 These figures have been culled from Zauba.com, a website that provides data on Indian exports and imports.

43 Joji Thomas Philip, Intelligence agencies fear China is trying to encircle India via tech deals with neighboring nations, *Economic Times*, 23 January 2013. Available online at http://articles.economictimes.indiatimes.com/2013-01-23/news/36505479_1_huawei-and-zte-nepal-telecom-telecom-and-internet-communication.

Chinese manufacturers have about 20% of the Indian telecom market while Indian telecom manufacturers have only 3% of the market. In some sectors such as 3G networks, this can go upto 60%. The Indian government asked a number of its agencies to analyze the risks involved and they reported back, highlighting various issues. One report said Chinese vendors were "supplanting and not supplementing" indigenous players in India's telecom equipment manufacturing sector. Another report highlighted vendors' reluctance to share technical information and system keys of their products with Indian operators. (A subsequent report noted that these key have been supplied to Indian companies.)[44] There have been a few instances of contracts being cancelled, but only with state run telecom companies.

4.4. Responses

4.4.1. *Implementing a national cybersecurity policy*

Cybersecurity has been within the purview of the National Security Council since 2002 with the National Security Council Secretariat taking many cybersecurity initiatives and participating in international dialogues. The role of the National Security Council Secretariat as the locus of any discussions on cybersecurity and for bringing together the various stakeholders has been honed to perfection. But it has been less successful in the natural corollary of co-ordinating the actions required to translate talk into action. While the need for a cybersecurity co-ordinator at the National Security Council Secretariat has been highlighted in successive reports, it is yet to be translated into action.

The government has been engaged in an intensive exercise to strengthen the country's cybersecurity,

44 Anupam Dasgupta, "Dragon in your dongle", *The Week,* 1 September 2012.

embarking on a multi-pronged strategy, first engaging closely with the private sector, as well as with international partners. However, regular revelations of such attacks by relevant agencies has had the effect of alerting the highest levels of government about the potential threats to critical infrastructure by such easy penetration of networks. A National Cybersecurity Policy that has a carrot and stick approach was released in July 2013 and since then has been proceeding in fits and starts. Despite the long gestation process, the policy was pilloried for falling short of spelling out concrete policies as well as for certain glaring omissions, such as the absence of a specific role for the armed services for ensuring India's cybersecurity.[45] In their defense, the National Security Council that has brought out the Policy has made the point that the NSCP is only one part of a 3-part framework including a National Cybersecurity Architecture and a National Cybersecurity Strategy. Even as the other two legs are awaited, the policy itself has been fleshed out through the promulgation of guidelines, beginning with the Guidelines for Protection of National Critical Information Infrastructure with guidelines for other sectors under production.

A national cybersecurity strategy would perforce fill in the many existing lacunae and gaps in thinking on cybersecurity within the country. Even if it does not resolve the tensions between the various interests and priorities of different groups, be it the private sector, law enforcement, or national security agencies, or even infosec professionals, it would try to balance all these requirements to arrive at a consensus that is palatable to all stakeholders. Secondly, it would also give a sense and direction on the overall vision which is lacking at present.

45 See Bhairav Acharya "The National Cybersecurity Policy: Not a Real Policy" *ORF Cyber Monitor,* vol. 1, no. 1, August 2013. Available online at http://orfonline.org/cms/sites/orfonline/html/cyber/cybsec1.html. Accessed on 23 September 2013.

4.5. Creating an institutional framework

An overarching framework is being created with various agencies apportioned different responsibilities. A National Cyber Coordination Center (NCCC) is being set up for threat assessment and information sharing among stakeholders, a Cyber Operation Center to be jointly run by the civilian authorities and the armed forces for threat management and mitigation for identified critical sectors and defense, and a National Critical Information Infrastructure Protection Center (NCIIPC) are some of the agencies created. In addition the military has also been proactive in creating a Cyber Command a long the lines of those created in other countries though there has been little discussion on the contours and responsibilities of such a Command.

The Computer Emergency Response Team-India (CERT-IN) began operations in 2004 with a mandate to "create a safe and secure cyber environment through appropriate policies and legal frameworks". Specific tasks included creating appropriate cybersecurity standards/guidelines, auditing, networking and points of contact, conducting cybersecurity drills, devising and deploying Crisis Management Plans and Cyber Alert systems, and interfacing with Sectoral CERTS, and Foreign CERTS. The Mumbai Attacks of 1998 which were considerably cyber-enabled from conception to implementation prompted the Government to amend the IT Act in that year itself.[46] The Information Technology Amendment Act, 2008 provided for a national nodal agency for critical information infrastructure protection which was set up after it was decided to make the NTRO the nodal

46 Investigations revealed that the terrorists had used Google Earth used for training, VOIP to communicate with their handlers, and Garmin GPS units and satellite phones were also found in their possession.

agency for critical infrastructure.[47] Section 70 of the IT Act, 2000 defines critical information infrastructure as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety". The National Critical Information Infrastructure Protection Center (NCIIPC) was established under the National Technical Research Organization in 2013, almost five years after being incorporated in the IT Amendment Act, 2008. The increasing instances of state sponsored malicious activities would have been a factor in the creation of this organization and situating it within the NTRO.

The organization's official mandate is to "Protect critical infrastructure against cyber terrorism, cyberwarfare and other threats". In pursuit of this mandate, it has been given all powers necessary including interception powers. Oversight is provided by an Advisory Council of 17 representatives from different agencies. Among the sectors identified as critical by it are civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, communication, information technology, law enforcement, intelligence agencies, space, and government networks.

There are a number of potential obstacles to the effective working of the NCIIPC. Compared to CERT-In, it is much less public facing which can prove to be a problem in an environment where much of the infrastructure rests in private hands.

4.5.1. *Ensuring supply chain integrity*

In this unfolding situation that is marred by distrust, supply chain integrity has become paramount with the

47 "Five-year plan in the works to revamp cybersecurity", *Times of India*, 18 December, 2012.

needle of suspicion pointing towards the hardware and software that make up the brains and body of cyberspace. While much of the equipment used in global networks is supplied by China, the storage and data storage networks are largely the domain of first mover companies, based in the United States but are also dispersed across other developed countries. Many countries rely on trade control mechanisms, but such measures have fallen foul of trade treaties as well as the competitive prices offered by, particularly, the Chinese manufacturers.

The government has tried to use prescriptive policy measures to get companies to go down the referred path. The government in the National Telecom Policy of 2012 set a target for domestic production of telecom equipment to meet Indian telecom sector demands to the extent of 60-80 percent by 2020. The Ministry of Communications and Information Technology has repeatedly urged telecom companies to take note of vulnerabilities in their equipment and told them they would be held responsible and subject to penalties if the vulnerabilities are not addressed. Ironically enough, Huawei was the only company to come forward when the government invited companies to collaborate with the Indian Institute of Science in Bangalore to develop a testing lab to check telecom equipment for malware.[48] The issue is not so much about hidden backdoors and kill switches as widely reported in the press as the fact that network equipment providers get access to sensitive information in the course of providing after sales support. When the government tried to implement a Preferential Market Access Policy for telecom products, it was the western companies that protested through their

48 Bharti Jain, Home ministry may seek review of IISc-Huawei Pact to set up telecom lab, *The Economic Times*, 28 June 2011. Available online at http://articles.economictimes.indiatimes.com/2011-06-28/news/29722347_1_telecom-gear-chinese-telecom-telecom-equipment. Other companies did not come forward because of worries over intellectual property rights.

governments and forced the government to roll back the policy.[49]

The government is also promoting the establishment of fab manufacturing facilities within the country to the extent of providing seed money and facilitating strategic partnerships with global players.[50] In addition to reducing the dependence on imports, it is believed that having fab manufacturing facilties within the country would enhance the security of IT products since embedded vulnerabilities are virtually impossible to locate. Other lacunae that have been identified and are being progressively addressed include setting up a Center for Cryptology,[51] and further securing sensitive governmental networks.

4.6. Takeaways

Thinking on the strategic aspects of cybersecurity is still in its infancy in India, partly because of the complex nature of the medium as well as the fact that there have not been any major known attacks through cyberspace. Policy makers have largely concentrated on securing Indian cyberspace through a combination of policies; the National Cybersecurity Policy along with the National Telecom Policy

49 PMO Defers Extension of Policy of "preferential Market Access' to Private Telecom Operators." *The Economic Times*. 6 July 2013. Accessed on 18 November 2013. Available online at http://articles.economictimes.indiatimes.com/2013-07-06/news/40407662_1_new-telecom-policy-pma-provisions-digital-europe.

50 "India Setting up Cybersecurity Architecture: National Security Advisor." *IBNLive*. 22 January 2013. Accessed on 18 May 2013. Available at http://ibnlive.in.com/news/india-setting-up-cyber-security-architecture-national-security-advisor/317028-3.html.

51 "Government Announces Setting up of R C Bose Center for Cryptology– The Economic Times." *The Economic Times* 4 March 2014. Accessed on 4 May 2014. Available at http://economictimes.indiatimes.com/industry/et-cetera/government-announces-setting-up-of-r-c-bose-center-for-cryptology/articleshow/31421710.cms.

and the National Policy on Electronics as well as subsidiary policies such as the National Telecom Infrastructure Policy all contain prescriptions for securing cyberspace. Implementation of these policies has proved to be a hurdle, evident in the fact that many of these policies are more than a few years old, and implementation has progressed in a sporadic manner. In addition to the complacency brought about by the fact that there have been no major known attacks, the lack of urgency can also be attributed to the conflict between economic and security imperatives. This is best exemplified in the case study of China where the burgeoning needs of the Indian economy have nullified the warnings by the security and intelligence agencies of the inherent dangers in sourcing sensitive items from China. In point of fact, it is the recent revelations made by Snowden that have had a larger impact on Indian cybersecurity policy.

While the United States has been using those revelations to create the conditions for a cyber deterrence with China, there is no indication yet that China is ready to play ball.[52] They jury is also still out on whether deterrence is a viable concept in the context of cyberspace till such a time that both offensive and defensive capabilities have developed to the extent that they are an existential threat to states.

52 Farrell, Henry. "The Political Science of Cybersecurity IV: How Edward Snowden Helps U.S. Deterrence." *Washington Post*. The Washington Post, 12 March 2014. Accessed on 16 May 2014. Available online at http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/.

5

China and Southeast Asia: Offline Information Penetration and Suspicions of Online Hacking – Strategic Implications from a Singaporean Perspective

This is a most unusual chapter to compose, not the least because a Singaporean perspective is supposed to offer a window into China's interactions with its geopolitical neighbourhood, Southeast Asia. Yet, there are compelling reasons for doing so. Singapore is, by most measures of global connectedness, a First World hub of trade, information and finance in Southeast Asia. Moreover, Sino-Singapore relations have gained unprecedented momentum on a political and ideological plane compared to its ASEAN (Association of Southeast Asian Nations) neighbors. Finally, a small state perspective, such as Singapore's, can be treated as a bellwether of security in its immediate "regional international society". [CHO 06] A Singaporean perspective frames cybersecurity issues within a securitized frame of long term horizon forecasting, strategic anxiety and balanced appreciation of the political conditions of great and middle

Chapter written by Alan CHONG.

powers alike. In the area of cyber security, Singapore ranks amongst Asia's top three most densely Internet penetrated national societies, with South Korea and Japan sharing the other two positions.

On the subject of Southeast Asia, it is proposed that China-Southeast Asia ties in relation to the cybersecurity sphere follow two strategic patterns. In the offline sphere, China's foreign policy[1] actively practises soft power in the realms of diplomacy, economics, educational and cultural exchanges. We must not ignore the historical dimension to this plane of interaction. Flows of Chinese migrants, emotional ties between the "motherland" population and the diaspora in Southeast Asia, and the nearly continuous solicitation of moral support and funds for the remaking of feudal China into the modern world of scientific industry and political rights for the population all depended upon the Chinese migrants domiciled in Southeast Asia. In the post-Cold War present, there are also nascent bonds built upon limited amounts of political and security collaboration on a state to state level. In this short chapter, I will briefly account for this soft power dimension because it exemplifies the perspective put forth by Martin Libicki where the "conquest" of online politics is assured by open front activities that gain the target populations favor through tangible initiatives that deliver physical welfare to those populations. As Libicki put it:

1 I will treat "China" and its legal name the "People's Republic of China", or "PRC", synonymously as the same nation-state. The descriptor "Chinese" may occasionally refer to the cultural nation of persons of Chinese ethnicity regardless of domicile, such as in reference to the Chinese diaspora in Southeast Asia.

> Lost in [the] clamour about the threat from hackers is another route to conquest in cyberspace, not through disruption and destruction but *through seduction leading to asymmetric dependence*. The seducer, for instance, could have an information system attractive enough to entice other individuals or institutions to interact with it by, for instance, exchanging information or being granted access. This exchange would be considered valuable; the value would be worth keeping. Over time, one side, typically the system owner, would enjoy more discretion and influence over the relationship, with the other side becoming increasingly dependent. Sometimes the victim has cause to regret entering the relationship; sometimes all the victim regrets is not receiving its fair share of the joint benefits. But if the "friendly" conquest is successful, the conqueror is clearly even better off.[2]

This is soft power as foreign aid, and foreign aid becomes associated synonymously with a "good community" that acts as a generous and humane donor. [CHO 07] [NYE 04]. It is expected that if efficaciously delivered, such foreign aid engenders a positive predisposition to open information operations conducted by the People's Republic of China (PRC) in foreign territories since the PRC will be theoretically viewed by the foreign publics as a non-hostile intervener in local political economy. In fact, if we treat China's information penetration as legitimate interventions in political economy, there is no "politicizable" issue with the PRC's open intelligence gathering until some egregious violation is broached in the mainstream media. China's information penetration is assumed to be synonymous with

2 [LIB 07] p. 3. Italics mine.

what I have termed "information operations", which refers to that entire range of symbolic resources straddling both military and civilian spheres that are aimed at achieving national objectives in both peacetime and wartime [CHO 13].

In the online sphere, China-Southeast Asia ties register comparable levels of public concern with hacking, cyber vandalism and online information theft. While this has evolved into a matter of high political significance on the plane of Sino-US and Sino-EU relations, it must be borne in mind that the responses of Southeast Asian citizens and governments are divided by the goodwill generated in the offline sphere of practical soft power delivery by both the Chinese government and its citizens. Moreover, Southeast Asian netizens have also demonstrated in recent years a number of potential retaliatory capabilities in the online sphere from virus launching to the spontaneous articulation of disapproval of Chinese actions through blogs, Facebook and Twitter. Figure 5.1 summarizes the two-pronged organization of this chapter.

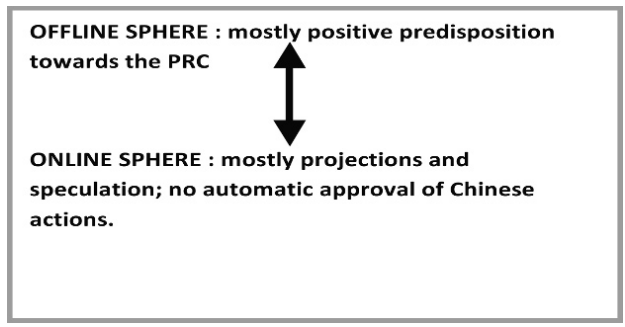


Figure 5.1. *Interactions between Offline and Online Predispositions towards Chinese Information Penetration*

The remainder of this chapter will thus devote considerable attention to how the People's Republic of China enjoys the latent offline privilege of tapping into an

intricately large information resource that is the overseas Chinese diaspora in Southeast Asia, and augmenting this resource with the formal deployment of soft power at the government-to-government and bilateral corporate levels. Offline information power is relevant in relation to comprehending the Chinese *interpenetration* of Southeast Asian states and societies since it fleshes out Libicki's thesis about the openly "seductive" dimension of the conquest of cyber spatial interactions. Online interactions between Chinese government proxies, spontaneous netizens and their counterparts in Southeast Asia do exist, except that they are not widely founded upon hard incontrovertible evidence, resembling instead much of the ephemerality and intangibility of cyberspace derived community. After probing both offline and online planes of China-Southeast Asia interactions, the chapter will conclude by calling attention to the need to frame research on China's so-called cyber-threat potential to Southeast Asia and the world in a more nuanced manner that takes into account other dimensions of Chinese information power rather than just cybersecurity or cyberwar potential.

5.1. Offline sphere: latent "diasporic" information power and official Chinese soft power

The starting point of discussing Chinese soft power in relation to China-Southeast Asia relations must begin with treating the Chinese diaspora in the Southeast Asian region as a large networked mechanism of information exchange. It may serve as a latent power extension for Chinese foreign policy and national security interests overseas. It might also serve as a network of divided loyalties and contradictory emotions that frustrates Chinese official policy implementation. A diaspora is commonly understood to be a collection of persons identifying with a particular ethnicity, religion or nationality who are domiciled outside their territories of ancestral or legal origin for reasons of work,

physical displacement arising from natural calamities, or of matters of political conscience. In this regard, as Leo Suryadinata observes, the phrase used to describe the Chinese diaspora in Southeast Asia, "Overseas Chinese", "has been used to refer to both Chinese nationals overseas and ethnic Chinese who are citizens of other countries. It also has the connotation that the Chinese are sojourners who will eventually 'return' to China". Moreover, "the term, often regarded as the English equivalent of a Chinese term *huaqiao* (Chinese sojourners), had been used before the problem of nationality arose during which the boundaries between Chinese overseas and local citizens were not clearly drawn"[3]. For the purposes of my argument, the "overseas Chinese" pose two implications. Firstly, Chineseness may be regarded as a state of mind and action regardless of one's physical domicile. Therefore, it is common to find the Chinese diaspora frequently referring to their cultural kin across Southeast Asia and those living in China itself for reaffirmation of cultural rituals, educational exchanges and exercises in linguistic proficiency.[4] Cultural Chineseness, as manifested in language immersion programmes, consumption of food and audio-visual popular programming and so on, reveal a thick volume of symbolic exchanges to reaffirm a common bedrock of cultural identity. Secondly, this also implies that persons identifying with the idea of cultural Chineseness would have developed either formal or informal networks of interaction whereby one segment of the Chinese diaspora in Southeast Asia may refer to another segment for expressions of moral, cultural or material support on the basis of retaining their collective cultural Chineseness. All these offline interactive features are relevant as information power features since they offer China a means of disseminating particular views about cultural authenticity, ideological correctness or variation, or

3 [SUR 85] p. 1.
4 [CHA 13] pp. 2–6.

simply articulating the parameters of Chinese patriotism.[5] In some ways, this is the phenomenon identified by Canadian media theorist Marshall McLuhan as the "tribalism" in communication facilitated by an electronically networked "global village": "it helps to know that civilization is entirely the product of phonetic literacy, and as it dissolves with the electronic revolution, we rediscover a tribal, integral awareness that manifests itself in a complete shift in our sensory lives"[6]. Therefore, by logical extrapolation, the diaspora offers a very appropriate *milieu* through which the "open conquest" of cyberspace occurs through the seductive appeal of affirming and re-affirming a common culture. However, we must also bear in mind that this diasporic information resource may be a fickle one subject to the contingencies of political and historical currents. Completing his study in 1985, Leo Suryadinata warns that:

> Southeast Asian nations, especially ASEAN, are still at the nation-building stage. Southeast Asian governments have adopted various measures in order to form their "national identity". Ethnic Chinese minorities have been quite responsive to these measures and the Southeast-Asianization of ethnic Chinese in this region will continue. The process is by no means smooth, especially in some countries where the government requires complete eradication of "Chineseness".
>
> With the exception of Indochina, many Chinese in Southeast Asia have been aware that their prosperity and safety depend largely on the local authorities rather than on Beijing or Taipei. This

5 [CHA 13] pp. 15–18.
6 [MCL 68] pp. 24–25.

> is especially so with Taipei which has no power to give meaningful protection to the ethnic Chinese.[7]

As a manifestation of this local Southeast Asian appreciation of the political correctness of "sanitizing" cultural Chineseness in relation to Beijing's potential diasporic network power, prominent local businesspeople in Indonesia, Thailand, Philippines, Vietnam and Cambodia have adopted names according to the indigenous national language, or have stylized their spellings to accord with local customs. It is a well-known fact that any form of ethnic Chinese deviation from local Southeast Asian nation-building projects would trigger either orchestrated reprisals in the form of the imposition of extremely discriminatory national policies, or organized rioting against Chinese persons and property in the urban areas, with the rare exception of Singapore, a state where ethnic Chinese form a clear majority. The reprisal scenario proved to be the reality in Indonesia under President Suharto in the 1980s, and post-unification Vietnam in the 1970s. Post-independence Malaysian politics have always witnessed the playing of "the Chinese card" by Malay Muslim politicians to win votes. On several occasions in the 1960s, this baiting of the Chinese boiled over into riots in Malaysia, consequently provoking the introduction of legislation to curb Chinese political and economic ambitions. As a result, ethnic Chinese businessmen in Malaysia and Indonesia have been visibly supportive of their governments' policies towards trade and investments with the PRC, and have commensurately aligned their political views in tandem with their governments postures towards China during the Cold War, after the Cold War, and on the occasion of the many rows over human rights practices between China and ASEAN on the same side, and the USA and EU on the other, in the 1990s and beyond. During the Asian Financial Crisis in 1998, anti-Chinese

7 [SUR 85] p. 23.

looting and rioting in a few Indonesian cities drew verbal condemnation from Beijing. Reciprocally, and quietly, ethnic Chinese businessmen in Southeast Asia have welcomed China's ascent as an economic powerhouse, notwithstanding the occasional social frictions between the PRC Chinese understanding of managed free enterprise economics and the more *laissez faire*, efficiency-driven, and market-friendly mindset of the overseas Chinese in Southeast Asia. It was no surprise that the Chinese in Southeast Asia have steadily supported Beijing's image burnishing efforts in the staging of the 2008 Olympics in the Chinese capital, and quietly shared Chinese netizens outrage at the 1999 "accidental" bombing of the PRC embassy in Serbia during NATO's humanitarian war in Kosovo [FUL 08]. Since the Deng Xiaoping reforms stemming from 1978, the PRC has especially courted Southeast Asia's ethnic Chinese businesspeople to invest in the "mother country".

Therefore, we might argue that the reliability of the Chinese diaspora as the PRC's information platform is a "half empty, half full" proposition, but the numbers of the diaspora, insofar as we count points of opinion as virtual ammunition in a war of public opinion in the era of global information flow, is considerable should the elites in Beijing attempt to cultivate it for foreign policy and national security purposes. Figure 5.2 provides a simple illustration of the number of "potential" pro-Beijing opinion points, sympathy conduits, and informal cyber "*gendarmes*" if Beijing can convert them to its side on any given issue. The statistics also reveal that the Chinese diaspora in Southeast Asian states is more numerous than those resident in the major western states such as Canada, the US and the UK. This may incidentally be construed to mean that Beijing may even dispense with cyberhacking as a means of ferreting valuable information from Southeast Asia, given the possibility of recruiting and mobilizing conventional spies. Conversely, if we take Libicki's arguments about the open

conquest of cyberspace seriously, then the Chinese diaspora in Southeast Asia might also be tapped as a resource available for infiltrating western centers of high technology. This can only happen if, and only if, Beijing's strategic planners can convert them into patriotic agents for its national security given the diaspora's dilatory relations with the central government in Beijing.

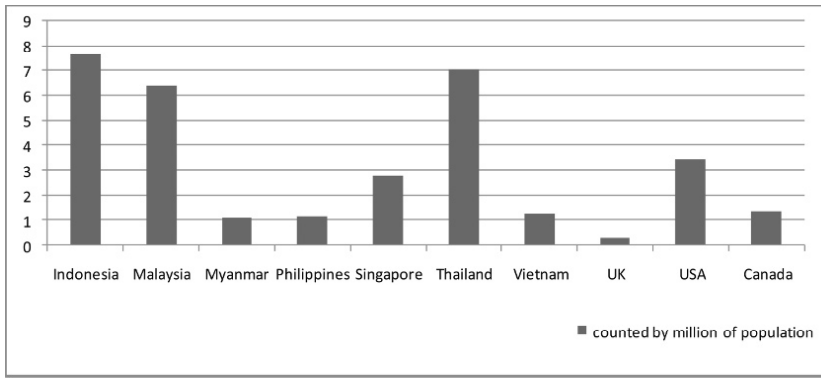


Figure 5.2. *The Chinese Diaspora in Southeast Asia Compared to the UK, USA and Canada. Source: [TEC 11]*

On the official level, Chinese soft power is an essentially post-Mao policy departure. During the Cold War, Chinese economic power overseas was thwarted by communist-inspired dogmatism at home and foreign policy abroad. China tried to employ networks of Chinese culture and education, such as cultural troupes, party officials and overseas Chinese medium universities in Southeast Asia, to act as proxies for spreading Maoist style revolution. This damaged China's soft power for decades. It was only with the advent of Deng Xiaoping's modernization programmes at home that foreign policy began to be re-aligned to support domestic development priorities. Having been made aware that Chinese political, diplomatic and cultural soft power towards Southeast Asia was tarnished by Beijing's Cold War strategies, the new leadership replaced their Southeast Asia

policy from the mid-1980s with foreign economic policy instead.[8] While Beijing initially welcomed trade and investment from the newly industrializing economies of Southeast Asia, from mainly Singapore, Malaysia, Indonesia and Thailand, the flow of trade and investment from the PRC to these countries equalized by the mid-1990s. China began to officially formulate aid packages for the reformist communist governments in Cambodia, Laos and Vietnam, and sought to offer foreign direct investment in the rest of the ASEAN economies on a win-win basis. China in turn needed alternative oil, gas and other energy supplies from Southeast Asia.[9] Finally, it was perceived that China's military and diplomatic interests could not be treated separately from the pursuit of a good neighbour policy towards Southeast Asia. Since 2005, ASEAN has emerged as China's fourth largest trading partner after the EU, the US and Japan. China had in turn attained in 2005 the position of being ASEAN's sixth largest trading partner.[10] Since 2011, ASEAN has become China's third largest trading partner, with forecasts by Chinese observers predicting that the number one position awaits in 2015 [BAO 12]. One way of viewing the size of Chinese soft power investments in Southeast Asia is to highlight a sample of its headline-making investments, as seen in Table 5.1.

Project	Country	Type	Cost	Company
LNG for Shanghai	Malaysia	Energy	US$25 billion	Petronas (Malaysian state-owned company)
Second Penang Bridge	Malaysia	Bridge	US$800 million	Export Import Bank of China

8 [HAA 05] pp. 112–115.
9 [SCH 08]; [CHA 13] pp. 7–13.
10 [SCH 08] p. 28.

High-speed train link (between both)	Thailand	Rail	US$4 billion	Chinese government
Electricity sold	Thailand	Electricity	US$2 billion	Sinohydro Corporation
LNG to Fujian	Indonesia	Energy	US$8.5 billion	British Petroleum (UK company)
Improve airport/seaport facilities in Papua	Indonesia	General infrastructure	US$930 million	China National Property Administration Council & Qili Holdings
Railway linking Luzon and the South	Philippines	Rail	US$400 million	Chinese government
Northrail Project	Philippines	Rail	US$500 million	China National Machinery and Equipment Corporation
Development Assistance (2003)	Burma	Aid	US$200 million	Chinese government
Oil Fields	Burma	Energy	US$163 million	CNOOC or SINOPEC
Stung Tatay Hydropower Plant (2006)	Cambodia	Energy	US$540 million	China National Heavy Machinery Corporation
Grants and Loans (April 2006)	Cambodia	Aid	US$600 million	Chinese government
Nam Ou VII Hydropower Plant	Laos	Energy	US$700 million	Sinohydro Corporation

Bokeo 168-Mw Hydropower Plant	Laos	Energy	US$340 million	China Southern Power Grid
Ninh Binh Fertilizer Plant	Vietnam	Agriculture	US$900 million	Wuhan Engineering Company and China National Machinery Corporation
Cao Ngan Thermal Power Plant	Vietnam	Energy	US$710 million	Harbin Power Engineering Company
Environment-ally-friendly Mixed/Coal-fired Tembusu Multi-Utilities Complex (Power Plant)	Singapore	Energy	US$1.6 billion	Huaneng Power International
Contractor & supplier for end-to-end network solution by the Nucleus Connect consortium to develop Singapore's Next Generation Nationwide Broadband Network	Singapore	Telecommunica-tions; digital infrastructure includes open access FTTP network, using GPON, Ethernet access technology and multi-service MPLS IP core technology to deliver bandwidths ranging from 100 Mbit/s to 1 Gbit/s	[Cost not reported]	Huawei Technologies

Steel, Aluminium and Palm Oil processing plants in Kuantan Industrial Park	Malaysia	Heavy and light industries	US$3.4 billion	Guangxi Beibu Group
Turnkey contract with PT Telekomunikasi Indonesia (PT Telkom) for a submarine cable known as "Mataram-Kupang" (MKCS) network	Indonesia	Telecommunications; cable has a designed capacity of 40 Gbps; stretching 1,200 km, the cable will connect five islands in the east of Indonesia, delivering broadband services and 3G services	US$138 million	Huawei Marine Networks
Donation of 171 computers to the Lao Ministry of Public Security (MOPS) to enhance Laos" cyber crime prevention capacity	Laos	Telecommunications; information security (sic)	[Cost not specified]	ZTE Corporation in association with the Chinese Embassy in Laos

Table 5.1. *The PRC's Key Infrastructure Projects and Investments (1990-2013)*[11]

While this list should be regarded as a mere snapshot of the entrenched nature of Chinese soft power in Southeast Asia, and hence not necessarily exhaustive, a number of strategic implications can be drawn in relation to cybersecurity in Southeast Asian national contexts. Firstly,

11 The bulk of this table was provided by Prashanth Parameswaran's published research article, especially Table 4.7 [PAR 10] pp. 43–44; also [HPI 13]; [OND 09]; [RAM 13]; [EKH 09]; [XIN 13].

Chinese state-linked companies and government departments enjoy direct access to the blueprints for the electrical, digital and electro-mechanical control systems of these infrastructure projects since the former are either the creators or collaborators in the design of infrastructure. This significantly eliminates the costs associated with disabling a potential adversary's infrastructure if the need arose in the context of acute hostility between the PRC and an ASEAN state. Secondly, a technological and infrastructural interdependence has arisen between local infrastructure users, governments and Chinese state-owned firms. Local users in Southeast Asia depend upon either Chinese training or Chinese maintenance. Local job creation by these infrastructural projects also engenders interdependence by way of skill transfers, and possibly, some degree of indirect and direct salary payments. And thirdly, the very threat of Chinese technical withdrawal during the partial completion and post-completion phases may be credible in inducing China's Southeast Asian collaborators to play ball with existing projects. Ultimately, it must surely be understood by all parties to these infrastructural projects that all modern infrastructure, including "brick and mortar" categories like power plants, optical fiber cables, steel factories and refining complexes, are heavily reliant upon IT circuits and their associated software. This creates cyber vulnerabilities for China's possible exploitation if relations turn hostile bilaterally. The telecommunications infrastructural projects in Indonesia, Laos and Singapore are the most prominent objects of the PRC's cyber "conquest" of Southeast Asia since the latter produced, either in whole or in part, the blueprints for digital connectivity. This digital infrastructure is almost always of a dual-use nature, offering both benign and malevolent possibilities for the PRC's long distance penetration, and should it be needed, sabotage. To date, neither ASEAN nor the PRC have even remotely speculated on these dark scenarios, despite the occasional public brushes with allegations of electronic espionage conducted by

the US and its collaborators within Southeast Asia that were unveiled by the disclosures of the American fugitive spy Edward Snowden from his refuge in Russia in 2013.

On the political and diplomatic front, the PRC has carefully avoided the ideological approach of the Cold War. Since the 1980s, Chinese diplomacy and security approaches to Southeast Asia have struck a pragmatic, neoliberal and functionalist tone, notwithstanding the unresolved disputes with ASEAN over the South China Sea (i.e. the Spratly and Paracel Islands) [HAA 05]. Table 5.2 summarizes the highlights of the PRC's current pragmatic soft power diplomacy.

Type	Description	Examples	Countries involved
Ideological security	China frequently defends a relativist standard of human rights for Asia. This reinforces the collective stance of ASEAN and most Central and South Asian states as well. In this way, China and its Asian partners join forces in fending off western scrutiny and sanctions over pereived violations of a "universal standard" of human rights	Outflanking western humanitarian ideas during the Asian Values debate 1992-2000; especially shielding Myanmar from intensified EU and US sanctions on human rights, etc.	All ASEAN

Agreements/ Forums	Signing treaties, organizing forums to promote "peaceful rise"	SEANWFZ, Treaty of Amity & Cooperation, Boao Forum	All ASEAN
Port Calls/ "Goodwill Visits"	Mostly naval ships docking in ports for friendly visits	E.g. two PLA ships dock in Changi Naval Base, Singapore	All ASEAN
Aid, Grants	Financial assistance for capacity-building (But this was somewhat dented by Beijing's dilatory and relatively miserly response to the victims of Typhoon Haiyan in the Philippines in 2013)	E.g. US$2 million for anti-Bird Flu programmes in Indonesia	Indonesia, Burma, Laos, Cambodia, Philippines
Technical Assistance	Providing technology or equipment to boost country programmes	E.g. 1,000 motorcycles to Indonesian police, satellites to Burma to battle drug trafficking	Indonesia, Burma, Laos, Cambodia

Educational Exchanges	Officer exchange or language programmes in military institutes	Thai officials attending courses at National Defence University, Beijing	Most of ASEAN
Joint Exercises	Holding combined military activities or attending others	ASEAN observes "Iron Fist" in China; "Strike 2007" takes place between Chinese and Thai armed forces; rest of ASEAN navies and armies have conducted varying degrees of limited map exercises or naval passing exercises	Most of ASEAN
Joint Training	Participation in combined training exercises, intelligence sharing and patrols	Laotian officials receive drug control training, China-Philippines joint detective unit	Most of ASEAN

Joint Policing against Non-Traditional Security Threats	Diplomatically amicable Chinese coordination of efforts to capture and try a drug lord who robbed and massacred 13 Chinese crew in October 2011 on two Chinese merchant ships on the Mekong.	Laotian, Thai and Myanmar officials received Chinese intelligence and in turn fostered camaraderie in a joint operation to nab the offenders. Laotian officials are encouraged by Beijing to claim credit for the drug lord's arrest and eventual extradition to China in 2012.	Laos, Thailand, Myanmar
Peacekeeping/ Volunteer Deployments	Providing personnel to assist in technical assistance and policing	INTERFET for East Timor, volunteer teams in Laos	Laos, Burma, Indonesia

Table 5.2. *Elements of China's Soft Power Diplomacy and Security Confidence-Building Strategy (1990-2013)*[12]

12 Information derived mostly from Table 4.12 of Parameswaran's 2010 study ([PAR 10] pp. 49–50) and updated by the author of this chapter based upon his own research [CHO 04].

A number of implications can therefore be drawn from this spate of soft power diplomacy. Firstly, the PRC is clearly manifesting a "charm offensive" by portraying itself as a practical, non-ideological partner of Southeast Asian states. Secondly, China is treating Southeast Asia as a demonstration zone for proving its claim to be a "peacefully emerging" responsible great power. This carefully cultivated image has been partially dented by the recent 2010-14 flare-up of the unresolved confrontation between China and its Southeast Asian neighbors over conflicting claims on the Spratly Islands. This heightening of maritime tensions between the Philippines and China cast a shadow over the Chinese response to the aftermath of Typhoon Haiyan which struck a large swath of the central Philippines in November 2013. Beijing's initial offer of US$100,000 in humanitarian aid was widely mocked in regional and international media even though it upped the amount to US$1.6 million within days. In comparison, Britain announced more than US$32 million, the US with US$20 million, and Japan with US$10 million [JAC 13]. Nonetheless, the overlapping patterns of pragmatic functionalist cooperation remain in place. Southeast Asian states do rely on Chinese cooperation in combating transnational corporate, maritime and financial crimes. Southeast Asian states also welcome China as a source of food imports as a substitute for inadequate homegrown produce. Moreover, China-ASEAN industrial zones offer complementary advantages for both their own MNCs and third party MNCs for co-locating manufacturing, research and development, and headquartering activities. China is therefore likely to be perceived as both a soft aid giver, and a practical partner in development. Thirdly, and finally, ASEAN states value a Chinese political and economic presence in the region as a buffer, or fallback, in the event of the political retreat of, or frictions with, western powers. China's growing political heft makes it an unspoken counterweight to American unilateralism on a variety of matters, especially on human rights and technology transfer.

For these reasons, China's offline diplomatic activism pre-empts somewhat any notion of the PRC as a cyber threat of the first order.

5.2. The online sphere: hacktivism as mostly projections

Chinese cyber-attacks within or targeting Southeast Asian societies are not well documented, but this does not mean that they do not exist. One Philippine academic has nonetheless documented a highly suspected PRC-sponsored cyber-attack on the University of Philippines website on 20 April 2012, whereupon the University's site was defaced. The next day, Filipino netizens affiliated with "Anonymous Philippines" retaliated against selected PRC websites.[13] In Singapore, Malaysia and Indonesia, there are reported instances of commercially targeted cyber-attacks on a frequent basis but there has been no direct attribution to the Chinese. In keeping with the carefully hedged analysis of this chapter, this author can therefore mostly project Southeast Asian capabilities *vis-à-vis* potential and actual Chinese doctrines.

To begin with, Southeast Asian cyberactivism can be traced to the following activities. Firstly, there is widespread evidence of nationalist cyber retaliation through blogging, Facebook, Twitter and other social media sites.[14] This phenomenon tracks the offline nationalistic sensitivities between Southeast Asian peoples whenever territorial claims are openly debated, or public slights are perceived by either side in any politicized issue ranging from food culture, to economic inequities between states, to personal blogs about a host society's discrimination against foreign students, to

13 [GOM 13] p. 256.
14 See for instance the evidence of Vietnamese bloggers retaliating against Chinese aggression in a third party online report at [HAY 12].

providing succour to unpopular dissidents from another state. This habit of protest and complaint increasingly takes on racist tones as online spats between Singapore and Malaysia, Indonesia and Singapore, Malaysia and Indonesia and Sino-Singapore people-to-people ties demonstrate in recent years [TEA 12]. Netizens, who are mostly within the 16-49 age category, are quick to take umbrage at national losses of "face" and to manifest it even before their respective foreign ministries produce an official reaction. On their part, Chinese bloggers active on their domestic Twitter and Facebook-like sites *weibo* and *sina.com* are also not reticent when it comes to polishing China's image overseas, especially if it requires intervention on third party hosted pages [TSO 13].

Secondly, some Southeast Asian states have on their statute books strict laws against sedition, propaganda actions contrary to public order, libel against sitting Heads of State and acts of *lèse majesté*. Thailand has been at the forefront of efforts to curb access to YouTube on the grounds of certain uploaded videos being deemed insulting to the Thai monarch. In the wake of the 1998 Asian Financial Crisis, Malaysia has instituted a net patrol unit to trawl Malaysian websites for seditious material assessed to be prejudicing economic recovery and regime stability. Ever since the Web arrived in Singapore, the government has practised strict vigilance against libellous comments against the sitting Cabinet members of the ruling party and launched legal actions against posters of racist commentary. It was only in 2011 that a ban on political campaign videos was lifted to facilitate "Internet-era" elections. Although it was not stated officially, the Barack Obama Internet election campaign of 2008 may have converted some officials in Singapore. Even freewheeling, democratic India had seen fit to take a leaf from Southeast Asian practice in August 2012 to force the closure of 245 websites that featured doctored visual media fanning anti-Muslim riots in the north-eastern

parts of the country. On that occasion, India formally pressured Google, Facebook and Twitter to aid in censorship for the sake of public order and social harmony [BAJ 12].

Thirdly, the boom in Facebook, Twitter and online shopping membership and activities in Southeast Asia have fostered national online civil societies that occasionally prove rambunctious and independent of their sovereign governments wishes. This "safety valve" allows dissent to flourish where offline political spaces are closed. This is the case across all of Southeast Asia. Online shopping itself generates a new sphere of consumerist loyalty that transcends national borders and may indirectly facilitate liberal "contamination" from the western consumer centres in the G7 economies. For instance, it is difficult to avert your gaze while shopping for iPads, fashionable garments, books and bags online while Amnesty International or Oxfam flashes paid advertisements promoting particular causes at the top of your shopping page, and some of these causes may well be endorsed by leading music and fashion celebrities, thereby subtly augmenting transnational cultural and ideological "contamination" from the perspective of sovereign authorities.

Finally, it needs to be noted that available academic and quasi-academic literature on Chinese cyberconflict doctrine produced in Southeast Asia tends to track western interpretations of Chinese capabilities and intentions with few exceptions. One Filipino assessment described Chinese cyber-strategy as largely manifesting low impact cyberconflict (LICC) with reference to the fact that the Chinese officialdom can wage "quiet war" or "retaliation" with impunity since the electronic consequences are mostly ephemeral with no loss of lives involved. This Filipino observer described LICC as "cases of cyber conflicts that are aimed towards influencing or shaping public opinion within the target state" and cites a Chinese military author as

stating that LICC is akin to metaphorically forcing a cat to consume hot pepper whereby the most subtle and least painful method is to "ground the pepper up and spread it on his [the cat's] back, which makes the cat lick himself and receive the satisfaction of cleaning up the pepper"[15]. The relative difficulty in confirming the identity of the source of a cyber-attack allows, in some Southeast Asian perceptions, Chinese hackers to get away with officially-sanctioned retaliation. This author's own reading of the few Chinese tracts on cyberconflict strategy online supports the view that the People's Liberation Army may be strategically avoiding an over-obsession with techno-electronic warfare aspects of waging cyberconflict in favor of amplifying its propagandistic aspects [PRC 08] [WAN 03]. The more important priority in a holistic conflict strategy is to seed doubt in the enemy's mind and then defeat him without physical combat, or at the very least, with the minimal clash of arms. This is an assessment also congruent with the author's own reading of Sun Tzu, Mao Zedong and Vo Nguyen Giap in establishing an Asian perspective on information operations [CHO 13].

5.3. Conclusion: offline politics strategically obscure online projections

In the light of present trends, circa 2014, we cannot conclude that the PRC poses a cyber threat to Southeast Asia in a definitive manner. The gains of Chinese soft power in the offline sphere ensure that China remains in the public eye of Southeast Asian societies as a mostly pragmatic partner in development and security confidence building. Nonetheless, there are possibilities that Chinese investments in Southeast Asian infrastructure and in the loyalties of the Chinese diaspora, may presage a more aggressive cyber strategy in the indeterminate future. The

15 [GOM 13] pp. 254–255.

online sphere seems to reveal an environment of latent threat potential from Chinese cyber capabilities but these largely remain projections in the absence of mounting evidence of Chinese cyber-attacks in the region. What is probably of more concern in the Southeast Asian cyberconflict arena is the pattern of nationalistic and inward-oriented possibilities for causing bilateral and domestic mischief against a developing nation's social harmony. The key to reading China-Southeast Asian cyber interactions has to lie mostly in performing offline sociological and political trend analysis for now. Therefore, the jury is either out on China's cyber threat to Southeast Asia, or the Chinese have taken to heart Libicki's thesis of openly propagated conquest of cyberspace through offline and online measures; or thirdly, and perhaps more culturally, the Chinese have adhered to the best parts of their strategic culture to wage conflict short of physical war through information operations.

5.4. Bibliography

[BAJ 12] BAJAJ V., "Internet Analysts Question India's Efforts to Stem Panic", *International New York Times*, August 21, 2012. http://www.nytimes.com/2012/08/22/business/global/internet-analysts-question-indias-efforts-to-stem-panic.html?adxnnl=1&adxnnlx=1392026755-BVU3UB/jIw8quv1vQWUqVQ (acces.sed)

[BAO 12] BAO CHANG., "ASEAN, China to become top trade partners", *chinadaily.com.cn,* April 20, 2012. http://www.chinadaily.com.cn/cndy/2012-04/20/content_15094898.html.

[CHA 13] CHANG A., Beijing and the Chinese Diaspora in Southeast Asia: To Serve the People*,* NBR Special Report #43, Seattle: National Bureau of Asian Research, pp. 1–30, 2013.

[CHO 04] CHONG A., "Singaporean foreign policy and the Asian Values Debate, 1992–2000: reflections on an Experiment in Soft Power", *The Pacific Review* 17, pp. 95–133, 2004.

[CHO 06] CHONG A., "Singapore's foreign policy beliefs as "Abridged Realism": liberal and pragmatic prefixes in the foreign policy thought of Rajaratnam, Lee, Koh and Mahbubani", *International Relations of the Asia-Pacific* 6, pp.269–306, 2006.

[CHO 07] CHONG A., *Foreign Policy in Global Information Space: Actualizing Soft Power,* New York: Palgrave Macmillan, 2007.

[CHO 13] CHONG A., "Information Warfare? The Case for an Asian Perspective on Information Operations", *Armed Forces and Society*, pp. 1–26, 2013.

[EKH 09] EK HENG, "Indonesia sizzles as market for China's telecom equipment makers; Huawei and ZTE Corp are integral to country's telecom sector", *Telecommunications International (TCIN)*, December 24, 2009.

[FUL 08] FULLILOVE M., "Chinese Diaspora Carries Torch for Old Country", *Financial Times*, May 19, 2008.

[GOM 13] GOMEZ M.A.N., Awaken the Cyber Dragon: China's Cyber Strategy and its Impact on ASEAN, 2013.

[HAA 05] HAACKE J., "The Significance of Beijing's Bilateral Relations: Looking "Below" the Regional Level in China–ASEAN ties", in HO K.L., KU S.Y.C., *China and Southeast Asia: Global Changes and Regional Challenges*, pp.111–327, Institute of Southeast Asian Studies, Singapore, 2005.

[HAY 12] HAYS J., "Dispute Between China And Vietnam Over The Spratly Islands And South China Sea", *FACTS AND DETAILS,* 2012. http://factsanddetails.com/china/cat8/sub52/item1902.html.

[HPI 13] HUANENG POWER INTERNATIONAL INC., "Huaneng Power International, Inc. Announces Operating Results for 2012", *Press Release – The Wall Street Journal – Asia Edition,* March 19, 2013. http://online.wsj.com/article/PR-CO-20130319-912822.html.

[JAC 13] JACOBS A., "Rivalries play a Role in Typhoon Aid", *International New York Times*, November 16–17, 2013.

[LIB 07] LIBICKI, M.C., *Conquest in Cybersapce: National Security and Information Warfare,* Cambridge University Press, 2007.

[MCL 68] MCLUHAN M., FIORE Q., *War and Peace in the Global Village*, Bantam Books, New York, 1968.

[NYE 04] NYE Jr. J.S., *Soft Power: The Means to Success in World Politics,* New York, Public Affairs, New York, 2004.

[OND 09] OPTICAL NETWORKS DAILY, "Huawei wins Singapore Next Gen NBN end-to-end network solution contract + expands CDB credit line to $30bn", *OBSERV*, September 24, 2009.

[PAR 10] PARAMESWARAN P., "Measuring the Dragon's Reach: Quantifying China's Influence in Southeast Asia (1990-2007)", *The Monitor: Journal of International Studies* (College of William and Mary, USA) 15, pp. 37–53, 2010.

[PLN 06] PEOPLE'S LIBERATION ARMY NAVY (PLN) WANG P-J *et al*., 对网电一体战在信息化战场上的特点分析 A Publication of the PLA Navy Dalian War Studies Institute, 2006, paper no.116018. [Author's translation].

[RAM 13] RAMASAMY M., "China, Malaysia Plan $3.4 Billion Industrial Park in Kuantan", *Bloomberg News.* February 5, 2013. http://www.bloomberg.com/news/2013-02-05/china-malaysia-plan-3-4-billion-industrial-park-in-kuantan.html.

[SCH 08] SCHMIDT J.D., "China's Soft Power Diplomacy in Southeast Asia", *The Copenhagen Journal of Asian Studies* 26, pp. 22–49, 2008.

[SUR 85] SURYADINATA L., *China and the ASEAN States: The Ethnic Chinese Dimension,* Singapore University Press, 1985.

[TEA 12] TEMASEK TIMES, "Majority of Singaporeans want NUS PRC scholar Sun Xu's MOE scholarship to be revoked", *The Temasek Times,* February 25, 2012. http://temasektimes.wordpress.com/2012/02/25/majority-of-singaporeans-want-nus-prc-scholar-sun-xus-moe-scholarship-to-be-revoked.

[TEC 11] THE ECONOMIST, "Diasporas – Mapping Migration", *The Economist Online,* November 17, 2011. http://www.economist.com/blogs/dailychart/2011/11/diasporas.

[TSO 13] TSOI G., "Edit Wars" on Wikipedia over China topics", *International New York Times*, October 28, 2013: 16.

[WAN 03] WANG V.W.-C., "China's Information Warfare Discourse: Implications for Asymmetric Conflict in the Taiwan Strait", *Issues and Studies* vol. 39, pp. 107–143, 2003.

[XIN 13] XINHUA NEWS AGENCY, "Chinese company donates computers to bolster Lao cyber security", *Xinhua Electronic News (XHELEN)*, December 2, 2013.

6

Impact of Mongolia's Choices in International Politics on Cybersecurity

Mongolia is a very special nation in at least two respects: its geographical position, sandwiched between two giants on the international scene and in cyberspace – i.e. Russia and China, its two bordering states; the political choices made by the authorities, which have committed Mongolia to a process of coming closer to the Western world, in order to attempt to find a third channel, complementary to its dependence on Russia and China. In this context, faced with two major powers which have a far greater mastery of cyberspace – if only because of the existing networking infrastructures, the number of connections, number of Internet users, national industries – what possible pretentions could a modest-sized state have in that same cyberspace? Is it not totally subjugated to the pressure from its neighbors? Is it possible for it to develop independently, freely, and enforce its own sovereignty? Is that sovereignty not threatened by the cyber-operations likely to be carried out against it by the major powers? Is cyberspace really that space of emancipation, with a level playing field, which would enable actors with modest capacities to assert their own ambitions? Indeed, what weight could a modest-sized cyberspace hold in the

Chapter written by Daniel VENTRE.

evolution of a state's society, its economy, its international relations and its security and defense policies? What role can a state with only a modest cyberspace hope to play in the global cyberspace? In this chapter, we intend to look at the way in which cyberspace is changing in the relations between China and Mongolia.

6.1. Mongolia's cyberspace

Since the mid-1990s, the telecommunications sector has been reformed, partially privatized for landlines (the historical operator being Mongolia Telecom), and opened for competition for landlines and mobile telephony. The mobile telephony market has experienced major and rapid growth. In 2005-2006, two new mobile telephony licenses were granted to Unitel (for GSM) and G-Mobile (CDMA)[1], which now share the mobile telephony market with Skytel and Mobicom Corporation. Three WLL (Wireless Local Loop) operators offer mobile coverage of the entire territory for telecoms services: Skytel, Mobicom and Mongolia Telecom Company. In a country where the population is nomadic, and disseminated over a truly vast territory, with few hardwired telecom infrastructures, mobile telephony has become popular. The penetration rate of mobile telephony is now higher than 100% (3.375 million mobile telephones in 2012).[2] The growth of the Internet amongst the population is greatly constrained by the peculiarities of the situation (large territory, low population density). On a geographic level, the country has a surface area of around 1.6 million km^2, and a population of 2.7 million inhabitants. The country shares a 3543 km border with Russia, to the north, and 4677 km boarder with China to the south.[3] The population is made up

1 [http://www.internetworldstats.com/asia/mn.htm].
2 [https://www.cia.gov/library/publications/the-world-factbook/geos/mg.html].
3 [https://www.cia.gov/library/publications/the-world-factbook/geos/mg.html].

of a 95% Mongol ethnic group, with the rest being Turks, Chinese and Russians.[4] The population is identified both as Buddhist and nomadic.[5]

	Population of Internet users	Penetration rate	GDP/inhabitant (in USD)
2000	30,000	1.1%	410
2001	100,000	1.5%	500
2007	268,300	10.3%	1 503
2009	330,000	10.1%	1 560
2010	350,000	11.3%	2 027
2013[6]	520,000[7]		

Table 6.1. *Evolution of the population of Internet users. Table constructed from data published by the ITU*[8]

A study[9] of the social media (such as Voodoo.mn and Biznetwork.mn, both set up in 2009) indicates that as yet, they are not widely used by Mongolia's populace. The most widely used social networks are based abroad (e.g. Hi5.com and Facebook). Also, the high rate of use of Facebook makes Mongolia an exception in comparison to its two neighbors,

4 https://www.cia.gov/library/publications/the-world-factbook/geos/mg.html.
5 Kristian Feigelson, Mongolie : la démocratie nomade, *Études* 5/ 2003 (Volume 398), p. 597–607. URL: www.cairn.info/revue-etudes-2003-5-page-597.htm.
6 [http://www.budde.com.au/Research/Mongolia-Telecoms-Mobile-and-Internet.html].
7 The statistics can differ significantly. The figures published by the ITPTA (Space Program in Mongolia) in 2013 speak of 641,000 Internet subscribers for 2012, which represents a 40% increase on 2011 (457,000 recorded subscribers).
8 [http://www.internetworldstats.com/asia/mn.htm] (for 2000, 2001, 2007, 2009 and 2010).
9 Tian-Syung Lan, Chun-Hsiung Lan, Oyuntuya Tserendondog, "Analysis of social network sites diffusion in Mongolia", *African Journal of Business Management*, Vol. 5(23), pp. 9889–9895, 7 October, 2011, [http://www.academicjournals.org/AJBM].

which tend to use national solutions instead (VKontakte for Russia and Qzone for China).[10]

6.2. Cyberspace and political stakes

6.2.1. *Mongolia targeted by cyber-attacks*

The first cyber-attack in Mongolia seems to have recorded in 1995.[11] Since then, although the networks are as yet modestly developed, and the case of cyber-attacks are not widely referenced and documented (notably because of the absence of any national legislational framework sanctioning computer pirating[12]), the country's networks have been subjected to cyber-attacks. We can cite a few examples, such as the attacks (essentially website defacements) of servers in the government, in banks, in education.[13] For example, the national police website (police.gov.mn) was defaced on 18 February 2013 by the "Viru$ No!r", apparently as part of the "Op Myanmar" operation.

Mongolia was among the 60 countries affected by the "Lurid Down Loader" attack[14] revealed in September 2011.

The website of the Mongolian Liberal Union Party suffered service denial attacks between 10 and 16 May

10 *White Paper on ICT Development*, Mongolia – 2013, ITPTA, 2013.
11 [http://www.mad-mongolia.com/news/mongolia-news/%E2%80%9C every-day-mongolian-websites-are-hacked-by-the-dozen%E2%80%9D-7960/].
12 [http://ubpost.mongolnews.mn/?p=5561]. Mongolia's penal law does not sanction hackers, which creates favorable conditions for them to act with total impunity. The law prohibits the dissemination of pornographic content and defamation. However, the legal framework as yet remains relatively cursory in terms of the Internet.
13 [http://www.mad-mongolia.com/news/mongolia-news/%E2%80%9C every-day-mongolian-websites-are-hacked-by-the-dozen%E2%80%9D-7960/].
14 http://www.zdnet.com/russian-space-systems-hacked-in-lurid-attack-3040094018/.

2012.[15] Those responsible for the attacks originating abroad have not been caught.

Figure 6.1. *Defacement of the national police Website, 18 February 2013 by Viru$ No!r*

Figure 6.2. *Defacement of the Mongolian Liberal Union Party website*[16]

15 http://www.lupm.org/chinese/pages/120529c.htm.
16 Source: [http://www.lupm.org/chinese/Pictures/nmg/LUPM.jpg].

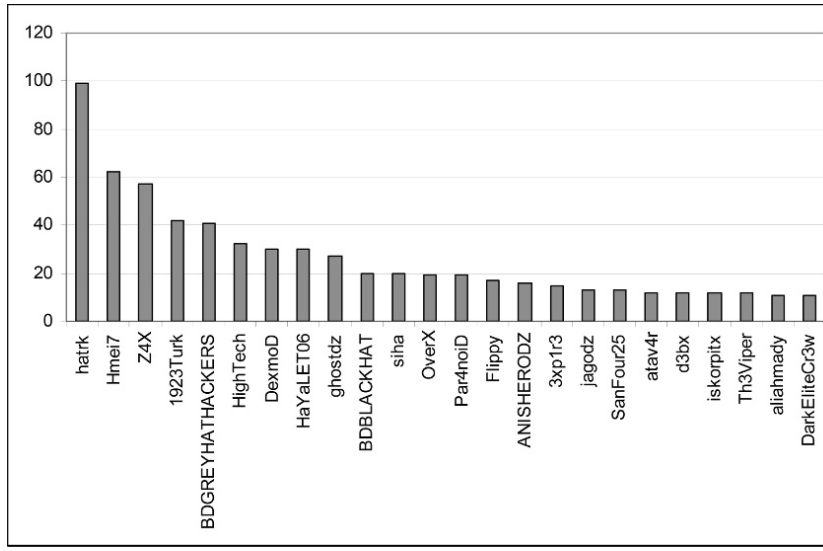


Figure 6.3. *Number of Mongolian websites defaced by each hacktivist signature, over the period from 8 June 2011 to 21 April 2014. Statistics established using data published on zone-h.org*

Over the period 8 June 2011 to 21 April 2014, the number of defacements of Mongolian websites, cataloged in the database zone-h.org, was 1250. The main signatures used were HaTRk (accounting for 26,674 website defacements to date by 23 April 2014); Hmei7 (264,000 defacements to his/her/their name); Z4X (171 defacements); 1923Turk (265,897 defacements); and BDGREYHATHACKERS (53024 defacements). These actors are not specifically targeting Mongolia's sites. Most .mn sites defaced are on Linux servers.

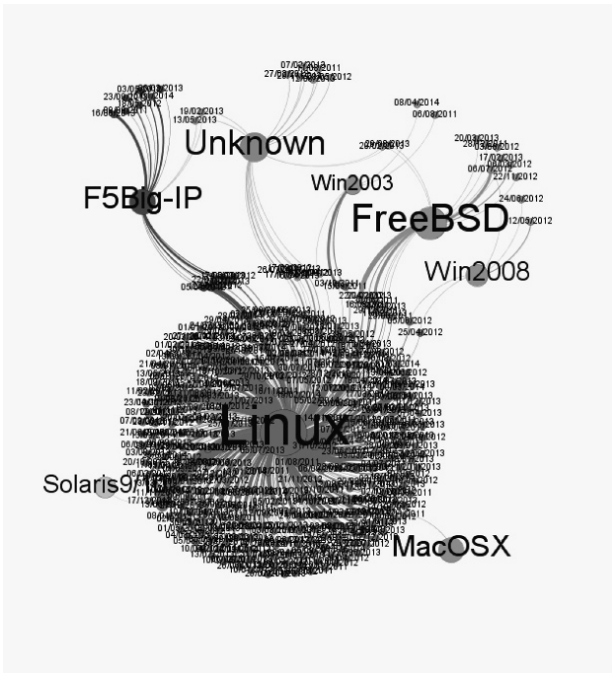


Figure 6.4. *Operating systems of the servers hosting the sites which have been defaced on the .mn domain over the period 8 June 2011 to 21 April 2014 (from the zone-h.org database)*

One of the reasons for the recent cyber-attacks suffered by Mongolia may lie in its changing place on the international chessboard, formalized by the opening up of the country to the West, thanks to the political willingness displayed by the government.

In 2011, Mongolia celebrated the 100th anniversary of its independence. In 1911, Mongolia was keeping its distance from China, before coming under Soviet control in 1924 (it was considered to be the "6th republic of the USSR"). On the political level, the fall of the communist empire gave way to a government of "communist" obedience, thus ensuring

continuity during the transition.[17] The country was governed by a communist regime, and then became a parliamentary democracy. When the Soviet Empire collapsed, Mongolia turned toward the Western democracies. It also began the process of development of its telecoms infrastructures.

The choice was made to forge closer links with the United States and the EU (but also Japan and other states) and break away from the lone influence of Russia and China – two giants on the international stage between which Mongolia is geographically pincered. In the 2000s, the ex-communist elites turned toward models of the market economy, toward America and Asia, i.e. new liberal democratic ideals.

The evolution of Mongolia's international position can be expressed in a variety of ways. Notable examples include:

– participation in joint military exercises, particularly with the United States: Khaan Quest 2013 (the 2014 exercise included participation from China);

– the signing of international agreements such as that linking Mongolia with the State of Alaska – more specifically the Alaska National Guard, as part of the National Guard Bureau's State Partnership Program, from 2003 onward.[18] Cybersecurity is one of the areas in which this exchange takes place;

– the increasing closeness to the EU can be traced back to 1989. An accord was signed with the EU in April 2013,

17 Kristian Feigelson, *Mongolie : la démocratie nomade, Études 5* / 2003 (Volume 398), pp. 597–607. [www.cairn.info/revue-etudes-2003-5-page-597.htm].

18 Kalei Rupp, *Department of Defense officials talk policy, cybersecurity with Guardsmen*, 3 May 2012, Office of Public Affairs, State of Alaska, [http://dmva.alaska.gov/content/Press_Releases/2012/Department%20of%20Defense%20officials%20talk%20policy,%20cyber%20security%20with%20Guardsmen.pdf].

relating to political dialog, trade, aid to development, cooperation in the domains of agriculture, energy, climate change, research and innovation, education and culture;[19]

– the "Electro Mongolia" (Tsakhim Mongol) program designed to develop ICT in the country has benefited from the support of foreign countries and international organizations[20]: South Korea contributing to the setting up of e-governance, the World Bank (which has been providing assistance since 2005)[21] and the Asian Development Bank[22] to the development of networks in rural areas, etc.;

– Germany has been one of the most active European partners in the aid given to Mongolia since 1991, particularly in terms of developing its telecommunications;[23]

– the European Union has permanent representation in Mongolia.[24] The action of the European Union and the finance from the assistance program go towards the diffusion in Mongolia of the norms and values held by Western society: democracy, human rights, environmentally sustainable development, equal access to healthcare, to education, social cohesion, defense of the most vulnerable, etc.;

– in terms of defense, NATO and Mongolia agreed on a cooperation program in March 2012.[25] Mongolia contributed

19 [http://eeas.europa.eu/mongolia/index_fr.htm].
20 *Mongolia – European Community, Strategy Paper. 2007-2013*, 23 February 2007, 42 pages, [http://eeas.europa.eu/mongolia/csp/07_13_en.pdf].
21 [http://www.worldbank.org/en/news/feature/2011/03/31/mongolia-information-and-communications-infrastructure-development-project].
22 *Country Strategy Paper (2002-2006) – Tacis National Indicative Programme (2002-2006), Mongolia*, 27 December 2001, 31 pages, [http://eeas.europa.eu/mongolia/csp/02_06_en.pdf].
23 *Country Strategy Paper (2002-2006) – Tacis National Indicative Programme (2002-2006), Mongolia*, 27 December 2001, 31 pages, [http://eeas.europa.eu/mongolia/csp/02_06_en.pdf].
24 [http://eeas.europa.eu/delegations/mongolia/index_en.htm].
25 [http://www.nato.int/cps/fr/SID-66692911-82159886/natolive/news_85430.htm].

to the operations in Afghanistan as part of the International Security Assistance Force (ISAF).

However, even with the proliferation of these exchanges, Mongolia is still heavily dependent on China: in 2007 almost 72% of Mongolia's exports went to China[26]; by 2011 that figure had risen to 92%. Russia, for its part, accounted for only 3% in 2007 and 2% in 2011. Also, this dependence on the Chinese market has seen constant growth in its absolute value, because the total amount of exports has tripled. In terms of imports, China was also Mongolia's main provider in 2011 (30%), followed by Russia (24%).

Cyber-attacks intended to spy on the Mongol government in 2013 were attributed to China. A recent attack credited to China has been analyzed by Threat Connect's Intelligence Research Team (TCIRT), which published its results in October 2013.[27] China is accused of using a cyber-espionage operation to try to learn more about Mongolia's relations with the European Union[28], the United States and other states such as South Korea and Japan. The attack took place through the dissemination of a compromised Word document[29] seeming to contain non-classified information about the Khaan Quest 2014 exercise (a joint operation between Mongolia and the United States), and to come from the United States Army Pacific (USARPAC) Unit. Opening the document triggers the installation and activation of a malware package. The perpetrators of the operation used a second document in the form of a false memo from the Mongolian Ministry of Defense, regarding an exercise with the Vietnamese army. The C2 servers used for the attack

26 Calculated using statistical data published on the site [http://mongolian embassy.us/about-mongolia/trade-and-economy/#.U3SOTfl_vX4]

27 7 October 2013. [http://www.threatconnect.com/news/khaan-quest-chinese-cyber-espionage-targeting-mongolia/].

28 http://www.threatconnect.com/news/khaan-quest-chinese-cyber-espionage-targeting-mongolia/.

29 "*DRAFT MSG – KQ14 – CDC ANNOUNCE* MESSAGE.doc".

were located in Hong Kong. The TCIRT investigation tracked the hack back to a young Chinese doctoral candidate at the Dalian University of Technology, named Yun Yan. The malware used also seems to have been employed by the hacker group APT1 analyzed in the Mandiant report in 2012.

6.2.2. *Nationalism on the Internet*

In Mongolian society, we are witnessing the emergence of anti-Chinese neo-Nazi movements, such as the group Tsagaan Khas ("White Swastika") founded by Ariunbold Altankhuum, or the groups Dayar Mongol or Blue Mongol. These movements are taking shape in a society with a poor economy, pointing fingers at those whom they believe to be responsible for their situations, first among which are foreigners – Chinese in particular. These ultra-nationalists describe themselves as patriots defending the rights of ordinary citizens against crime, inequality and corruption, drawing inspiration from Nazism (although they claim to reject the violence of Nazism), and referring to heroes from the country's history (such as Chingunjav[30] or indeed Genghis Khan – a legendary leader whose story was repressed during the Stalinist era, but who remains a hugely significant figure in Mongol culture[31]) to defend their national identity.[32] The demands of these ultra-nationalists relate to defense of the Mongol race, to fight against mixity, against the intrusion of China into the country, which perceived as an imperialist threat. The defense of the nation by these groups extends to protection of the environment

30 One of the two great leaders of the 1755-1756 rebellion, fighting for independence from the Manchus (China).

31 Genghis Khan's image is found on Mongolia's banknotes, and statues have been erected in his effigy throughout the country. In the neighboring countries, this cult is perceived as a resurgence of Mongol nationalism.

32 Tania Branigan, *Mongolian neo-Nazis: Anti-Chinese sentiment fuels rise of ultra-nationalism*, The Guardian, 2 August 2010, [http://www.theguardian.com/world/2010/aug/02/mongolia-far-right].

(fighting against pollution caused by foreign mining companies).[33] The members of the group Tsagaan Khas, which is seeking legitimacy and acceptation, appear to be adopting less violent practices in recent times. Yet they still act as militias, checking the operating permits of foreign mining companies, and patrolling the streets ensuring that Mongol girls do not have sexual relations with foreigners – particularly Chinese – (to keep the race pure). As is true the world over, these demands may be promulgated on Internet networks (for example, on YouTube). However, the actions and demands of these groups are causing waves and gaining widespread publicity in the reports made by the international media – particularly on the Internet.[34]

6.3. Information-space security policy

Conscious of the problems that cyberspace presents in terms of national security, but also probably at the urging of Western countries, the government has decided to implement a cybersecurity policy. Also, in order to drive forward measures to improve security in the country, Mongolia is and has been hosting international events relating to cybersecurity. On 27 January 2013, at the Defense University of Mongolia[35], a conference was held about the future of information technologies, with 26 participants. The 5th APT Cybersecurity Forum (CSF-5)[36] of

33 *A Mongolian Neo-Nazi Environmentalist Walks Into a Lingerie Store in Ulan Bator*, The Atlantic, 6 July 2013, [http://www.theatlantic.com/infocus/2013/07/a-mongolian-neo-nazi-environmentalist-walks-into-a-lingerie-store-in-ulan-bator/100547/].
34 For instance, see the reports published by western media: [http://www.theatlantic.com/infocus/2013/07/a-mongolian-neo-nazi-environmentalist-walks-into-a-lingerie-store-in-ulan-bator/100547/], [http://www.theguardian.com/world/2010/aug/02/mongolia-far-right], etc.
35 [http://www.dum.gov.mn/index.php?option=com_content&view=article&id=440%3A-2013-&catid=49%3A2011-02-08-05-45-33&Itemid=159&lang=mn].
36 [http://www.aptsec.org/2014-CSF5].

the Asia-Pacific Telecomm unity (APT) was held in Ulaanbaatar, 26-28 May 2014, under the aegis of the Information Technology, Post and Telecommunications Authority (ITPTA) (Mongolia). Thus, cybersecurity is now part of a national security program (strengthening of the security protocols on institutional networks, institutionalization of cybersecurity) but is also playing a part in Mongolia's international relations (prolonged international dialog by the organization of demonstrations on cybersecurity, facilitating debates and exchanges).

The government has adopted:

– the E-Mongolia National Program, defined by the Information and Communications Technology Authority (ICTA) for the period 2005-2012.[37] This is a roadmap set out by the government for the development of ICT in the country. The primary objective is to use NTICs as the basis for some of the development of the society and economy on the national information infrastructure, by offering an "*[equal], inexpensive, easy to use information communication service to all*". NTICs are perceived as the solution to numerous problems: "*Create open information environment that provides information on government, economy, education, science, art, literature, business sectors and society at large. Apply ICT advantages in order to eliminate corruption, bureaucracy and other impoverishments. Preserve Mongolian historical, traditional and societal wealth. Diminish poverty…*";

– the 312th Resolution of "Measures on providing state information security", in 2011. The Government Communications Department of the General Intelligence Agency was renamed the Cybersecurity Department, and its

37 *E-Mongolia National Program*, Information and Communications Technology Authority (ICTA), 3 pages, [http://workspace.unpan.org/sites/internet/Documents/UNPAN044899.pdf].

functions are to ensure the protection of the State's information and important information infrastructures, evaluate risks, managing the government's networks, and ensuring the integrity and security of those networks;[38]

– in 2010 the government approved the "*National Information Security Program*" (2010-2015). This document is the contemporary of a broad range of cybersecurity policies and strategies published in numerous countries, on all continents.

Information security is one of the six elements of this integral national security strategy[39]: "*National security shall be assured through the interrelationship among the "security of the existence of Mongolia", "economic security", "internal security", "human security", "environment security" and "information security";* " *The approach to security and action-making shall be based on knowledge, information and analysis."*

Information security is discussed in section 3.6: *"Information security: Assurance of national interests on information and guaranteeing information integrity, confidentiality and availability for the state, citizen and private organizations shall be a basis for ensuring information security".*

The text hinges around the following major arguments:

– the crucial importance of information security for national security;

– information and its security support national development (also note that, at least in the English-language

38 [http://www.infomongolia.com/ct/ci/3440].
39 *National Security Concept of Mongolia*, [http://mongolianembassy.sg/concept-of-national-security/#.U1e7tPl_vvY].

version of the document, the terminology used refers to information and information security, rather than "cyberspace", "cybersecurity" or even "information systems";

– the need to: *"3.6.1.2. Restrict outside entities' attempts to influence the social psychology, social stability and individual consciousness and ethics of Mongolians. Develop a capacity to disrupt or counter any information that promotes or supports animosity, discrimination or hatred and develop a social mentality of non-acceptance of such efforts"*. This focus on influence and social stability, and the fight against anything which could jeopardize peace in the heart of society, is highly reminiscent of the approach taken by its two neighbors, Russia and China, whose security strategies are designed to safeguard information security – Russia speaks not of cyberspace but of information space – and guard against outside influence which could disturb the peace and potentially give rise to interethnic, political (etc.) tensions in the country – this concern is shared by China and Russia;

– the Mongolian authorities are perfectly well aware of the possibilities of intrusion into the networks and the danger that could represent for the economy, security, and society;

– foreign enterprises in the domain of the Internet are subject to strict scrutiny. The State cannot and will not accept these media being used as a propaganda instrument by foreign powers: "*3.6.1.4. Rights of foreign-investment mass media activities in Mongolia shall be restricted if they harm national security. Ownership and association with media shall be transparent and their activities realistic, balanced and responsible. Support publication and promotion of national values through mass media and contain at proper level information on foreign religion, culture or state policy*". Thus, this policy entails the controlling of the activities of foreign media and of the content published;

– as in other states, including Western ones, the authorities have planned actions to raise social awareness of security issues: *"3.6.1.5. Develop a national policy on legal arrangement, standard, management, organization and training on information security to enhance social awareness and information security knowledge". "3.6.4.3. Establish a national security data base and develop a mechanism to provide citizens with wide-ranging information on national security through the State Great Hural, local government organizations and media. Maximize efforts to set up governance open information sources, methodologies and procedures to efficiently use these sources in the electronic governance services"*;

– information security concerns both the government and private enterprises. The approach needs to be all-encompassing and holistic, and the security organized (risk management, security audits, etc.);

– information security requires the existence of a pool of high-level professionals (but nothing is said about the way in such a resource is to be constructed. Will the engineers trained in Mongolia's own schools and universities have a sufficient level of expertise to satisfy the requirements?[40]);

– Mongolia touches on the debate about technological sovereignty, though that expression is not actually used in the text: *"3.6.1.9. Support and develop national manufacture of competitive information and communications systems,*

40 According to the *White Paper on ICT Development*, Mongolia – 2013 published by the ITPTA, in 2013, some 8023 people are employed in the NTIC sector: 7313 university students specializing in the following disciplines: software engineering, network administration, information systems and management, hardware engineering, telecommunications engineering, electronics engineering, optic communications, television and radio technology, satellite and wireless communications, and information technology.

equipment and software, develop solutions to national information security and reduce technological dependency";

– in order to constitute a recruiting ground of national experts in information security and of innovative engineers and entrepreneurs, the country needs to invest in high-level training, and in R&D. *"3.6.1.10. Specifically support national fundamental and applied sciences research, study and training on information and communication technology as well as information security"*;

– there is a focus on "cybercrime", but the first point in this brief discussion still stands. Indeed, this cybercrime takes place in a space which is not "cyberspace", but rather is "information space" – in other works the policy is essentially in line with the Russian concepts: *"3.6.1.11. Develop national capacity-building on computational forensics analysis to combat cybercrime or investigate, detect and collect evidence of crimes. 3.6.1.12. Develop and expand international cooperation to ensure information security, prevent the danger of confrontation in information space and combat cybercrime"*;

– a subsection is given over to *Integrity of information* (*3.6.2*). Thus, the document emphasizes quality of information and the risks of manipulation of information (rather than manipulation of data). Thus, there is a visibly more marked interest in information operations, and information warfare, than in the notion of cyberconflict as such: "*3.6.2.1. Integrity of information shall be ensured through protection of information, information space and infrastructure from illegal intrusion, manipulation or theft*";

– the solutions favored by the authorities are similar to those adopted in most States: ensuring specific protection of State data, State information systems, ensuring the security in the information infrastructures, putting in place a digital signature public key infrastructure, reducing the

vulnerabilities of the networks, systems, and sites, encrypting exchanges, etc.;

– public–private cooperation needs to be one of the driving forces of security;

– a set of specific measures (legislational, in particular) needs to define different categories of information, and different levels of classification;

– in this document, the main focus really is on the government's information, and on the data held by the State: "*3.6.3.2. Refine government information categorization and security classifications, improve legal environment for management and organization of classified information protection to a higher level*". The protection of personal data is also mentioned: "*3.6.3.7. Prohibit intrusion on individual or family privacy, correspondence, information confidentiality, rights and freedoms except in cases of ensuring national security and following all legal procedures*".

In 2012, the Ministry of Defense published the *Operational strategy of the Ministry of Defence*[41], which envisages the forces to be restructured and for them to employ new technologies. Cybersecurity is briefly touched upon in the paper, although no discussion is specifically dedicated to the issue. However, the army is facing the issue of cyberdefense, having itself fallen victim to cyber-attacks targeting it either directly or indirectly (see the cyber-attack as part of Khaan Quest 2014 mentioned above). Mongolia intends to profit from its cooperation with NATO to extend its cyberdefense activities.[42] Yet in spite of these new-found friends, Mongolia is not entirely breaking off its military

41 [http://www.legalinfo.mn/annex/details/5610?lawid=8768].
42 *NATO and Mongolia agree programme of cooperation*, 19 March 2012, [http://www.nato.int/cps/en/natolive/news_85430.htm?selectedLocale=en].

relations with China[43], as the mutual trust agreement signed in 2003 between the two countries was transmuted into a strategic partnership in 2011. China is Mongolia's economic and political partner, and remains so in spite of Mongolia's efforts to find a third neighbor.[44] The cyber-attacks in 2013 attributed to China are unlikely to jeopardize these relations.

43 Alicia J. Campi, *Efforts to Strengthen Sino-Mongolian Relations in Fall 2013*, China Brief Volume: 13 Issue: 24 December 2013.
44 Ganzorig Dovchinsuren, *Mongolia's Third Neighbor Policy: Impact on the Mongolian Armed Forces*, United States Army War College, March 2012, 40 pages, [http://handle.dtic.mil/100.2/ADA561642].

7

China-Iran-Russia – A Cybercommunity of Information?

In China, the proliferation of cybernetic attacks and counter-attacks, at first glance, looks like chaos caused exclusively by individual interests: kleptomaniacs steal data or paralyze their competitors, whilst private security companies try to keep them from doing so. On the face of it, this is the situation. However, if we dig deeper into the question, notably attaching credence to China's latest declarations, we see that many of the world's cyberconflicts take place across a dividing line, with the United States and their Oceanic allies on one side and three continental powers – China, Iran and Russia – on the other. This raises the following question: are China, Iran and Russia all individually and independently concerned with their cybersecurity, or is there actually some sort of cooperation between these states? The following viewpoint will be defended in this chapter: *China's cyberdefense strategy* is based increasingly on two Asiatic partners: Iran and Russia. This nascent cooperation results in the discreet emergence of a veritable community of information (or of disinformation, depending on the point of view). Indeed, China's cyber-strategy is inextricably linked to the increasing geopolitical

Chapter written by Thomas FLICHY DE LA NEUVILLE.

closeness of China, Iran and Russia. However, this strategic evolution should not be exaggerated, as the primary goal of Chinese cyberdefense is not predation, but rather the maintenance of internal order.

7.1. The hall marks of cyber-cooperation

In a domain which is supposed to be secret, it is possible to present two forms of evidence: circumstantial evidence based on implications, and proof in the only domain where publicity is required: that of cyber-information.

7.1.1. *Pax cyber-mongolica*

Cyber-attacks within the China-Iran-Russia space are limited. Although there has been a great deal of publicity about the *Iranian cyber army* which is believed to have attacked the Chinese search engine Baidu, it seems unlikely that the attack was orchestrated by Iran. Indeed, the search engine, which is close to the Chinese government, cannot really be held to have served as a relay for anti-Iranian material. On the other hand, it is known that there have been an increasing number of exchanges of researchers between China and Iran in the cyber domain in recent years. It must not be forgotten that on its border with Afghanistan, China has a Persian language-speaking minority whose engineers are perfectly capable of joining Iran's research programs. On the other hand, as these nations are growing closer in terms of energy supply due to sanctions, Chinese cultural centers in Iran have developed. The low number of cyber-attacks between China, Iran and Russia has also been noted by the United States, who fear what was indelicately called a "*cyber Pearl Harbor*", orchestrated by China, Iran and Russia. The United States, though, has a different cyber view of each of these three countries: China is thought to engage in rational stealing of American technology by sheer

effect of mass; Russia, the US' old adversary, is to be feared because of its creativity; Iran, for its part, seems to be an irrational cyber-actor, which urgently needs to be distanced from the other two master Asiatic powers.

7.1.2. *A cyber-community of information – the proof of Syria*

A cyber-community of information has been born; the Syrian conflict is the illustration of this. There is a true convergence of the views of the Iranian, Chinese and Russian press on the subject of the Syrian conflict. The *Syrian revolution* is perceived, on non-allied Internet networks, as an attempt to undermine Bashar-al-Assad's regime. The *Syrian opposition*, largely made up of foreign jihadists, is believed to be masterminded by the United States, Saudi Arabia and Qatar with the aim of sparking the collapse of the Syrian "dominoes". Russian sites deem it to be unacceptable that the opposition should be armed by the United States, and celebrate the arrival of Russian warships in the eastern Mediterranean. For their part, Iranian Websites say it is logical that Russia should come to Syria's aid, saying that support is based on the continuity of Russian policy. The Islamic Republic's Websites regularly report secret American military preparation in Jordan, with the aim of coming to the aid of the Syrian opposition. For their part, China's Websites make their positions known under the guise of neutrality, by alternating between quotes and comments. Chinese sites often repeat the declaration of Hillary Clinton: "*The United States will not intervene, and will only provide humanitarian aid*". *It is understandable* – added to low-level ill-feeling towards China on a daily basis – *that America has had enough of war and wants to concentrate on its own problems at home. The Americans do not want to be engaged in another war in the Middle East after Iraq and Afghanistan*". The People's Daily also relays

Bashar-al-Assad's declarations: "*I am not a puppet. I was not made by the West to go to the West or to any other country*". Put simply, although they couch their statements in caution, the Russian, Iranian and Chinese Internet networks openly support Bashar-al-Assad's regime.

7.1.3. *The counter-point of Mali*

On the other hand, the coverage of the crisis in Mali between 11 and 22 January 2013 reveals a difference of position between the Russian, Iranian and Chinese press apparatus. The Russian newspapers reacted very quickly, condemning France's intervention for a number of reasons: France was pursuing a neo-colonial policy in Africa, seeking to mine gold and uranium from West Africa. Also, it was still paying for its mistakes in Libya. By a curious paradox, in Mali, France was fighting the Islamists which it had supported in Syria. The war was hugely costly for France – around €400,000 per day. In addition, France did not have the forces needed to defeat the jihadists. Unlike what was being said in the Western press, the Tuaregs would absolutely not support their intervention. On the other hand, France would have to rely on the United States, benefitting from their aerial logistic support and their intelligence capabilities. In brief, behind the French operation could be seen the unmistakable profile of the "*FUKUS axis*", the inverted "axis of evil" denoting **F**rance, the **UK** and the **US** – powers who were seeking clandestinely to overthrow Russia. The Iranian press quickly took up the baton on most of Russia's criticisms, and added one rather cruel one: the French offensive seemed to be a misdirection ploy by the French President in order to turn public attention away from France's own internal problems. For their part, China's news websites remained reserved, contenting themselves with using quote marks to mark their disapproval: "*Last weekend, the air strikes by the Malian army, supported by French air strikes, "destroyed" a number of Islamist support bases in the*

north of Mali. These were "targeted" strikes. The authorities in these countries say they are convinced that there is strength in the union, and are expecting a "happy ending" from this "acting solidarity" over Mali". Thus, unlike Russia and Iran, therefore, the Chinese websites favored cautious, guarded coverage of the Malian issue. The reason for this is very simple: it is in China's interests for France to secure the Sahel to exploit the uranium mines in Niger. The treatment of these two crises by the Chinese, Russian and Iranian press is revealing of the different approaches taken by the three states.

Put briefly, the territory of the new Mongol Empire of China, Iran and Russia not only appears to be a space of cyber-peace, but also as a domain in which an information community has emerged. In actual fact, these cyber-realities are merely the reflection of the geopolitical relations of strength.

7.2. The geopolitical bases for the cyber-Mongol empire

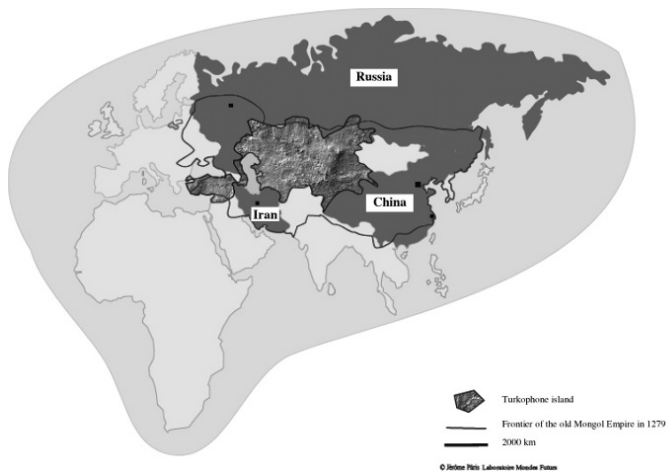


Figure 7.1. *The Turkophone island, key to control of the new Mangol empire*

7.2.1. *An undeniable closer Sino-Iranian relationship*

The relations between Iran and China are fluid and changeable, both for pragmatic and sentimental reasons. There is an underlying basis of common ground between the two countries, which leads to the development of their past, present and future relations. China and Iran are the heirs to two major civilizations, and the links between them go back to the Second Century BCE, when the Han Dynasty opened up the Silk Route. This trade route played a major role in the exchanges between the Hans and the Arsacid Empire.[1] In addition, whilst this route helped promote trade, it also encouraged cultural exchanges between the Persians and the Chinese for many centuries. This shared heritage of the Silk Route serves today as a historical link between Iran, Central Asia and China. These links are important, in that they are used by the Chinese and Iranian leaders to demonstrate friendship between the two nations, and also (on the contrary) to recall their unfortunate experiences and tense relations with the Western powers.[2] Iran and China share not only a common history, but also a profound sense of victimization and "humiliation" by the West.[3] These two countries feel themselves excluded from the regional and global politics practiced by the major powers. The discourse of victimization continues to play an important role in the rhetoric from the Chinese and Iranian authorities. China and Iran are deeply suspicious of the eventuality of a world order dominated by the United States, and are working to bring about a multi-polar worlds where American influence is diluted. During a visit to Iran in 1991, the Chinese

1 Also known as the Parthian Empire.

2 Ehsan Ahari, "China's Proliferation to North Korea and Iran, and its Role in Addressing the Nuclear and Missile Situations in Both Nation", U.S.-China Economic and Security Commission, 14 September 2006, http://www.uscc.gov/hearings/2006hearings/written_testimonies/06_09_14wrts/06_09_14_ahrari_statement.php.

3 John W. Garver, *China and Iran: Ancient Partners in a Post-Imperial World*, University of Washington Press, 2007, p. 285.

Premier Li Peng declared: "*we are opposed to the domination of the United States or of a minority over the rest of the world, and to America's building of a new order in international relations, and on this point we are in perfect agreement with the Islamic Republic of Iran*".[4] In June 2009, Hu Jintao reaffirmed this position, declaring that: "*Tehran and Beijing should work together to manage developments, on the international scale, which favor their nations, or else the very people who are the cause of the current international problems will continue to rule the world.*"[5] The Iranian leaders have, many times, demonstrated similar sentiments. The President of Iran, Mahmoud Ahmadinejad, has often spoken of the creation of "*a new world order*".[6] Russia, for its part, is becoming more and more sensitive to Western injunctions, and its good relations with Iran are darkening. In 2009, Russia expressed its displeasure at Iran's refusal to send slightly enriched uranium to Russia and France to be transformed into fuel for its reactor generating medical isotopes. Invoking the United Nations Security Council resolution of June 2010 forbidding all countries from supplying conventional weapons to Iran, Russia prohibited the delivery of S-300 missiles to Iran.[7] Moscow has also previously backed a series of UN resolutions sanctioning Iran.

4 John W. Garver, *China and Iran: Ancient Partners in a Post-Imperial World*, University of Washington Press, 2007, p. 107.
5 Ariel Farrar-Wellman and Robert Frasco, "China-Iran Foreign Relations", American Enterprise Institute, 13 July 2010, http://www.irantracker.org/foreign-relations/china-iran-foreign-relations.
6 "Ahmadinejad Stresses Need for New World Order", *Fars News Agency*, 07 June 2010, http://english.farsnews.com/newstext.php?nn=8903171502.
7 Fred Weir, "Why Russia is cutting off major arms sales to Iran", *The Christian Science Monitor*, 23 September 2010, http://www.csmonitor.com/World/Europe/2010/0923/Why-Russia-is-cutting-off-major-arms-sales-to-Iran.

7.2.2. *Arms sales in Russo-Iranian and Sino-Iranian relations*

The sale of arms to Iran by China and Russia, which all three countries believe to be legal, is a major source of discord between China/Russia and the United States. Russia remains Iran's main supplier. China also trades with Tehran in this area, and participates in exchanges of military technologies and materials which could be used for civil or military purposes.[8] In spite of thorny relations with Iran after the fall of the Shah in 1979, the USSR succeeded in selling arms to the Islamic Republic. In 1989, Moscow and Tehran negotiated their main armament contract along with the scientific and technical cooperation accords. Until the latter half of the 1990s, Russia had a stable position as Iran's main supplier of conventional weapons. Between 1995 and 2000, Russia suspended its arms sales to Iran in fulfillment of an agreement with the United States.[9] Over the first decade of the 21st Century, Russia sold over 5 billion dollars worth of military equipment to Iran, including Tor-M1 short-range anti-aircraft missiles, warplanes, submarines and armored vehicles.[10] Iran sought to obtain ballistic missiles, and in 2004 the US Secretary of State, Colin Powell, alerted the international community to the fact that Iran could try essayer to adapt nuclear warheads to fit ballistic missiles.[11] Iran was reported to be trying to develop a Shahab-6 missile – a variant of the North Korean Taep'o-dong-2C/3

8 Robert G. Sutter, *China's Rise in Asia*, Rowman and Littlefield Publishers, Inc., Maryland, 2005, p. 45.

9 Lionel Beehner, "Russia-Iran arms Trade", Council on Foreign Relations, 1 November 2006, http://www.cfr.org/iran/russia-iran-arms-trade/p11869#p3.

10 Fred Weir, "Why Russia is cutting off major arms sales to Iran", The Christian Science Monitor, 23 September 2010, http://www.csmonitor.com/World/Europe/2010/0923/Why-Russia-is-cutting-off-major-arms-sales-to-Iran.

11 Robin Wright and Keith Richburg, "Powell Says Iran Is Pursuing Bomb", Washington Post, 18 November 2004.

missile, with a range of over 5,000 kilometers. Moscow may have aided Tehran with technology transfers for this program, and even helped Iran to build a missile with a 10,000 kilometer range capable of reaching the east coast of the United States.[12] With regard to China, Beijing is known to have sold arms to Iran since the Iran/Iraq war from 1980 to 1988. Between 1980 and 1987, China is thought to have sent Iran armaments with a value of over 3 billion dollars.[13] After the war, arms sales fell, but the trade resumed at the beginning of the 1990s. From 1993 to 1996, China supplied weapons to Iran for a total of 400 million dollars, and 600 million dollars between 1997 and 2000.[14] It has been established that China was the second-largest supplier of arms to Iran between 2002 and 2011.[15] Many of these weapons are believed to be sophisticated, and potentially capable of doing damage to the American airforce and naval fleet. China has also transferred a range of industrial technologies to Iran, and in doing so, contravened its own laws on technology transfers and unilateral American legislation. Besides small-caliber weapons, China has supplied Tehran with artillery, anti-ship cruise missiles, surface-to-air missiles, fighter planes, tanks, armored

12 "Shahab-6/Simorgh-5, 6?", GlobalSecurity.org, http://www.globalsecurity.org/wmd/world/iran/shahab-6.htm, 26 January 2009.

13 Richard F. Grimmet, "Trends in Conventional Arms Transfers to the Third World by Major Suppliers: 1980-1987", Congressional Research Service, U.S. Government, p. 116, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497150&Location=U2&doc=GetTRDoc.pdf, accessed 21 March 2012.

14 Ila Berman, "The Impact of the Sino-Iranian Strategic Partnership", U.S.-China Economic and security Review Commission, 14 September 2006, http://www.uscc.gov/hearings/2006hearings/written_testimonies/06_09_14wrts/06_09_14_berman_statement.php.

15 Stockholm International Peace Research Institute, "Arms Transfer database", 21 March 2012, http://armstrade.sipri.org/armstrade/page/values.php.

vehicles for transporting troops and speedboats.[16] The Obma administration are thought to have concluded that Chinese companies were contributing to the development of missiles and the Iranian nuclear program, in violation of the sanctions imposed by the United Nations Security Council.[17]

7.2.3. *Sino-Russian support for Iranian civil nuclear development*

Other economic considerations guide both the Chinese and the Russians in their attitude to Iran. Over the course of the past decade, Russian and Chinese diplomats have tried, many times, to slacken the Security Council resolutions – particularly those which could restrict their economic collaboration with Iran – particularly in the field of energy. They have managed to preserve their economic interests in Iran, in spite of the UN's economic sanctions. In February 2010, Oleg Rozhkov, the Adjoint Chief of the Security and Disarmament Affairs Department in the Russian Foreign Ministry, declared that Russia would only abide by the sanctions against Iran which "*aim to solve the issues of non-proliferation and of Iran's nuclear program*". He also mentioned that Moscow was "*not going to work on sanctions or measures which could lead to the political or economic or financial isolation of this country*".[18] With the exception of the case of the S-300 missiles, the trade links between

16 Michael Mazza, "China-Iran Ties: Assessment and Implications for U.S. Policy", American Enterprise Institute, 21 April 2011, http://www.irantracker.org/analysis/michael-mazza-china-iran-ties-assessment-and-implications-us-policy-april-21-2011.

17 John W. Garver, "Is China Playing a Dual Game in Iran", Center for Strategic and International Studies, The Washington Quarterly, Winter 2011, p. 76.

18 Ralph Winnie, "Iran: Russia's Strategic New Client", *The Washington Post*, 22 March 2010, http://russianow.washingtonpost.com/2010/03/iran-russias-strategic-new-client.php.

Russia and Iran have not been greatly affected, and Russia is one of Iran's main suppliers.[19] Russian companies have assumed a leading role in aiding the development of Iranian civil energy, which also includes the nuclear sector. The building of the Bushehr nuclear power plant began in the 1970s under the Shah, and the project was then resumed many years later by the Russians. The plant officially began producing electricity in September 2011.[20] Having concluded an agreement with the International Atomic Energy Agency, Russia committed to make the plant operational, provide the nuclear fuel and recover the used fuel for the first few years of the plant's operation.[21] The Russians find it easier to cooperate with Iran in the development of its civil nuclear capabilities because they officially believe Iran does not intend to use its civil nuclear sector to produce a nuclear weapon. In December 2011, the Russian Vice Minister for Foreign Affairs, Sergei Ryabkov, declared: "*We have seen and verified data showing that there is no tangible evidence of the existence of a military component in Iran's nuclear program.*"[22]

7.2.4. *A clear-cut Sino-Russian diplomatic position on the Iranian program*

China and Russia are asking the Iranians to refrain from developing a nuclear weapon, and to be more transparent about their research efforts. At the same time, these two

19 Christian Caryl, "The Other Ticking Clock in Iran", *Foreign Policy*, 7 October 2009, http://yaleglobal.yale.edu/content/other-ticking-clock-iran.
20 "Iranian Nuclear Power Stations begins Generating electricity", *The Guardian*, 4 September 2011, http://www.guardian.co.uk/world/2011/sep/04/iran-nuclear-power-`hehr-plant.
21 "Iran Launches Bushehr Nuclear Power Plant", *Ria Novosti*, 12 September 2011, http://en.rian.ru/world/20110912/166785925.html.
22 "No military component in Iran's nuke program: Russia", *Xinhua*, 10 December 2011, http://www.china.org.cn/wap/2011-12/10/content_24122033.htm.

countries have often defended Iranian positions on the Security Council, and even cooperated with Iran in the nuclear domain. The Chinese and Russian diplomats note that the existing sanctions against Iran have not managed to persuade Iran to abandon its nuclear program, but instead have caused Tehran to become more deeply entrenched in its positions. They are calling for dialog and renewed efforts. In June 2010, on the Security Council, Moscow and Beijing sided with the West and voted for sanctions against Tehran, which was accused of carrying on its sensitive nuclear activities. These activities violate the previous Security Council resolutions, prohibiting Iran from enriching uranium or conducting other activities which could contribute to the development of its nuclear weapons, until Tehran exhibits more transparency in the context of its nuclear research.[23] This firmer attitude towards Iran on the part of the Chinese and Russians became clear when Russia and China refused Iran full member status in the SCO. They deemed that Iran could not benefit from that status as long as the country is subject to sanctions by the UN.[24] Neither China nor Russia want Iran to acquire a nuclear weapon, but both partners have always defended the right of Iran or any other country to carry out nuclear activities for pacific ends, such as energy production. In 2007, President Vladimir Putin summarized Russia's position concerning Iran: "*We have no evidence of Iran's intention to produce nuclear weapons. Therefore, we proceed from the premise that Iran has no such plans. But we share the concern of other partners and believe that Iran's programs must be transparent*."[25] In May 2008, in a shared

23 Richard Weitz, "Why China and Russia Help Iran", *The Diplomat*, 19 November 2011, http://the-diplomat.com/2011/11/19/why-china-and-russia-help-iran/.
24 "L'Iran peut adhérer à l'OCS si l'ONU lève ses sanctions", *Ria Novosti*, 13 May 2011, http://fr.rian.ru/world/20110513/189470063.html.
25 Richard Weitz, "Why China and Russia Help Iran", *The Diplomat*, 19 November 2011, http://the-diplomat.com/2011/11/19/why-china-and-russia-help-iran/2.

declaration, the Chinese Premier Hu Jintao and the Russian President Dmitry Medvedev affirmed that "*China and Russia propose that Iranian nuclear problem be resolved by dialog and consultation*."[26] In September 2010, China and Russia placed the emphasis on a long-term global solution which was necessary to "*restore the international community's confidence in Iran's peaceful use of nuclear energy*."[27] Following a tripartite meeting in November 2010, The Chinese, Indian and Russian Foreign Ministers once again recognized Iran's right to use nuclear energy for peaceful purposes.[28] In July 2011, China and Iran celebrated the 40th anniversary of diplomatic relations between them. China seized the opportunity to reiterate that it desires a peaceful solution to the Iranian nuclear problem.[29] The Russians and Chinese probably wish for a change of behavior from the Iranian authorities, although they are concerned about regime change in Iran. Were the Iranian opposition to come to power, it would certainly take a dim view of Sino-Russian support for President Ahmadinejad. During the demonstrations in 2009, the protesters vehemently criticized the Sino-Russian assistance to the Iranian regime. They also

26 "China, Russia rule out military actions on Iran", Chinese Government's Official Web Portal, 24 May 2008, http://www.gov.cn/misc/2008-05/24/content_990969.htm.

27 An Lu, "China, Russia call for increased efforts in Asia-Pacific security: joint statement", Chinese Government's Official Web Portal, 28 September 2010, http://www.gov.cn/misc/2010-09/28/content_1712083.htm.

28 "Joint Communique of the 10th Meeting of the Foreign Ministers of China, Russia and India", Chinese Government's Official Web Portal, 16 November 2010, http://english.gov.cn/2010-11/16/content_1746273.htm.

29 "China, Iran celebrate 40th anniversary of establishment of diplomatic relations", Embassy of the People's Republic of China in the Islamic Republic of Iran, 18 July 2011, http://ir.chineseembassy.org/eng/dtxw/t841539.htm.

reproached the Russians and Chinese for their rapid congratulations[30] to President Ahmadinejad after his election, which was contested by the opposition.

7.2.5. *Oil and gas at the heart of economic relations*

The Chinese, for their part, have benefited from a situation where few countries are trading with Iran. Thus, Chinese companies have managed to fill the holes in various sectors of the Iranian economy – particularly that of energy – left by Western companies. In 2009, China became Iran's main trading partner, ousting Germany, which had held the position up until then. Iran is not only one of China's main oil suppliers, but is a crossroads for energy transport between the Middle East, Central Asia and Europe. Their relationship remains asymmetrical, mainly because of Iran's economic isolation: Iran needs China more than China needs Iran. Since the 1980, China's relationship with Iran has evolved from the trading of weapons to the trading of energy, to support China's uncontainable economic growth. The numerous sanctions imposed by the United States and other Western countries against Iran have forced the Iranians to turn to the East to find outlets for its abundant energy resources. In its quest for energy to feed its development, China has often sought to exploit the opportunities in place which others have neglected or turned away from. The American and European companies have been turned away or have left, and the Chinese took advantage of the opportunity to take their place.[31] The Chinese and Iranian governments played a crucial role in cementing the energy partnership. Iran is aware that Chinese companies can put

30 Natalya Shurmina and Guy Faulconbridge, "Russia and China congratulated Iranian President Mahmoud Ahmadinejad on Vote Win", *Reuters*, 16 June 2009, http://www.reuters.com/article/2009/06/16/us-iran-president-sb-idUSTRE55F0YA20090616.

31 Jean-Pierre Cabestan, *La Politique internationale de la Chine*, Presses de la fondation nationale des sciences politiques, Paris, 2010, p. 370.

in investment, and the Iranian government offers incitements to attract new investors. During his tour of the Arabian Peninsula in January 2012, the Chinese Premier Wen Jiabao declared, in response to the threat to close the Strait of Hormuz, that "*China is not the only country trading with Iran*", and that China had no concerns about trading oil with Iran.[32] At the same time, Chinese oil companies have the indulgence of Beijing, enabling them to pay lesser administrative charges and benefit from rates on finance for their projects which are lower than the market rate.[33] China is seeking to diverse its suppliers, and the links it maintains with oil- and gas-exporting countries. Iran remained one of China's main oil suppliers, through 2009, 2010 and 2011.[34] China not only buys crude oil from Iran, but involves itself upstream and downstream in the production process through investment. Upstream (early in the process), China has become involved in prospecting and production of crude oil. Since 2005,Chinaand Iran have signed numerous accords in the energy sector, involving the three main Chinese companies: China National Petroleum Corporations (CNPC), Sinopec, and China National Offshore Oil Corporation. In 2007, Sinopec and the National Iranian Oil Company (NIOC) signed a two-billion-dollar agreement for the exploitation of the Yadavaran oil field, with a production capacity of 300,000 barrels of oil per day.[35] Its downstream investment

32 "Pékin continue de commercer avec l'Iran", *Le Figaro*, 19 January 2012, http://www.lefigaro.fr/flash-eco/2012/01/19/97002-20120119FILWWW00378-pekin-continue-de-commercer-avec-l-iran.php.

33 Peter Mackenzie, "a Closer-Look at China-Iran Relations", *CNA China Studies*, September, p4, 2010. http://www.cna.org/sites/default/files/research/D0023622%20A%20Closer%20Look%20at%20China-Iran%20Relations.pdf.

34 Judy Hua and Chen Aizhu, "Update 1-China's Jan crude oil imports from Iran down 14 pct m/m", *Reuters*, 21 February 2012, http://www.reuters.com/article/2012/02/21/china-iran-oil-idUSL4E8DL0FM20120221.

35 "China's Sinopec, Iran ink Yadavaran deal", *Chinamining.org*, 11 December 2007, http://www.chinamining.org/Investment/2007-12-11/1197342543d8153.html.

is in oil refining and distribution of crude oil products. Chinese investors have conducted negotiations to develop the refineries at Anahita, Abadan, Shiraz and Isfahan.[36]

Cooperation between Iran and Russia in the energy domain goes back to 1916, when the Iranian government offered a concession to a Russian merchant. More recently, in 1970, the trans-Iranian pipeline, 1,106 kilometers long, was commissioned to link the Soviet Union to Iran. It was the first Iranian gas pipeline devoted to export. In 1972, gas exports rose to 8 billion cubic meters.[37] In 1972, a treaty was signed, authorizing the Soviet Union to engage in the development of Iranian gas and oil, along with petrochemical industries and electricity plants. In December 1976, an agreement was signed between Iran and the USSR to export natural gas from Iran to Germany and France through Soviet territory.[38] The Iranian revolution in 1979 and the invasion of Afghanistan by the USSR's troops had a considerable effect on the relations between the Iranians and the Soviets – all the more so because the USSR supplied arms to Iraq during the Iran–Iraq conflict. Exchanges in the energy sector were tentatively resumed at the start of the 1990s. Over the course of the next 20 years, cooperation in that sector did not experience phenomenal expansion. Although Iran and Russia have considerable energy reserves, they are not able to conclude a true partnership in order to hold greater sway over the international energy market. In July 2010, the Russian Energy Minister announced the launch of a massive program of cooperation with Iran in the field of oil, natural gas and the

36 Sadeq Dehqan, "7 Refineries to Go Private By Yearend", *Iran Daily*, 30 August 2011, http://www.zawya.com/story.cfm/sidZAWYA20110830044957.

37 Mandana Tishehyar, "Iran-Russia Energy Relations", *Iran Review*, 8 July 2011, http://www.iranreview.org/content/Documents/Iran_Russia_Energy_Relations.htm.

38 *Ibid*.

petrochemical industry.[39] In December 2011, Russia and Iran signed a contract relating to oil with a value of over a billion dollars. That contract, signed between the oil company Tatneft and Iranian Petroleum Engineering and Development Company, envisages developing the Zageh oil field in the Iranian province of Bushehr on the coast of the Persian Gulf. This collaboration should be able to deliver a production rate of over 55,000 barrels per day by 2016.[40]

A new Mongol Empire has thus been born, but for a variety of reasons, China, Iran and Russia are in no danger of reconstituting the Mongol Empire of Antiquity which federated them. Unlike in the 13th Century, today these three civilizations actually encircle the Turkish community, which previously brought them together, as a sort of "island": China is pursuing its policy of confining the Turko phone minorities to Xinjiang; Russia is having trouble containing the Altaic peoples of Caucasia; Iran, for its part, views Turkey as a rival power in the region. Secondly, all three countries suffer from a structural demographic weakness, which is likely to prevent them from exercising power in the long term. In spite of these weaknesses, the cultures in these states offer an exceptional capacity for innovation. Thus, the Mongol Empire could be reborn today, in the form of a very pragmatic alliance between three powers in whose interests it is to support one another. The materialization of such an alliance is something the United States fears; the united states' best tactic, indeed, involves keeping those states divided. In spite of its attempts, however, an alliance has taken shape. In 2001, China and Russia founded the Shanghai Cooperation Organization, one of the main objectives of which is to counter American influence in

39 Andrew E. Kramer, "Russia Plan to Help Iran Challenges Sanctions", *The New York Times*, 14 July 2010, http://www.nytimes.com/2010/07/15/world/europe/15russia.html.
40 "Iran, Russia ink $1bln worth of oil deal", *Xinhua*, 19 December 2011, http://www.china.org.cn/world/2011-12/19/content_24190611.htm.

Central Asia. Tajikistan is another of the founding members. It was joined by Iran in 2005 and Afghanistan in 2012. This means that the whole of the Persian-speaking world now belongs to that alliance. Including 1.5 billion inhabitants over 26 million square kilometers, the Shanghai Cooperation Organization has at its disposal 50% of the world's uranium and 40% of the world's carbon supply. It is in this context that joint military maneuvers have been carried out, along with exchanges in the fields of medicine and nanotechnologies. The new Mongol Empire therefore cannot be viewed as a dead zone in the inexorable march toward pacifying globalization: hence, this alliance is founded on shared geopolitical interests, promoting a world vision that runs counter to the stereotypes held in the West.

7.3. Order in cyberspace: an absolute necessity within China

It would be misguided to approach a discussion about China as though it were a country like any other, ultimately destined to be part of the inevitable peaceful, globalized Utopia. From a purely industrial standpoint, China is naturally looking to conquer the markets, but in light of its 4000-year history, this is a relatively secondary objective. In addition, during the Renaissance era, although its own ships absolutely dwarfed the tiny Portuguese caravels, China made no attempt to seize the overseas territories that it explored. In reality, far more than control of the markets, China is concerned primarily with its internal unity. The domain of cyberconflict, though, is no exception to the rule.

7.3.1. *Interior order and exterior disorder*

The Chinese strategies are, to a large extent, determined by China's astronomical number of inhabitants. In China, innumerable people may be in agreement over even the

slightest decision; their chain reactions are concomitant to their phenomenal collective "mass". Even when faced with apparent disorder, therefore, it is helpful to preserve a level of order which nothing can overthrow. The old or new Mandarins present themselves as the ultimate guardians of order. In addition, the administration's absolute dominance over the populace has, for centuries, relied on the existence of an inspection body. Consider the example of the strategically important province of Tibet: China's primary water source and a strategic observation post looking over China and India, Tibet has been kept weak for centuries by the theocracy of the monks. This space is particularly sensitive from the cybernetic point of view. Pro-Tibet sympathizers outside of China (human rights organizations or pressure groups, for example) have been the target of cyber-attacks. In addition, China has announced the launch of an Internet- and phone-monitoring program affecting 4 million users. What is true for Tibet is also true for Xinjiang: it is imperative to preserve internal order, in the face of the risk of implosion – internal order must be preserved at all costs. With external order, it is a different matter. At any rate, the issue is not a new one. The question was once put by Louis XV to an old Jesuit returning from China. He narrowed his eyes a little and responded: "Sire, I shall merely quote what one of the Emperor's counsellors once said to him: *'The barbarians are like animals, and absolutely should not be governed in the same way as the Chinese are. If we try to control them using the maxims of good reason, only trouble will come of it. The old kings understood that, which is why they ruled the barbarians by means of disorder. Therefore, governing the barbarians through disorder is the true* way*, the best way, to govern them'"*. At the time, this answer raised a great many eyebrows in society. Yet after all, what is a cyber-attack if not ruling by means of disorder?

7.3.2. *The appearance of peace and the necessity of secrecy*

The major advantage of a cyber-attack is that it fits in perfectly with a fundamental tenet of Chinese culture: the desire to preserve the outward appearance of peace. In China, the never-ending quest for peace stems from the ancient philosophical schools of thought, born in the troubled times of warring kingdoms. Thus, counter to the heroism of a Greek warrior, celebrated by the populace before being channeled by the Church, runs the Chinese celebration of the pacific sovereign. In that context, open warfare is perceived as a senseless and extravagant act – losing touch with reality. Hence, apparent peace is preferable to the unleashing of violence and proof of truth by the sword. The exaltation of peace has gradually metamorphosed into a "quest for harmony" in China's official discourse. The upshot is this: the best cyber-attack would be one which goes unnoticed. Massive-scale cyber-attacks (such as those favored by Russia) are to be avoided, in favor of cyber-harassment. Finally, the culture of secrecy fits in well with the emergence of cyberconflict. In order to effectively combat the centrifugal forces threatening China, it is wise to preserve secrecy. Dissimulation is the normal way of behaving in society. Whilst this makes it difficult to shed light on the way in which China defends itself against cyber-attacks, the strategy is definitely not uncoordinated: its defense system is hybridand decentralized, and therefore perfectly equipped to deal with the threats at hand.

In brief, as we can see, the defense of domestic order at the risk of exportation of chaos involves the promotion of harmony and secrecy. Above all, China's cyberdefense is intended to safeguard Chinese unity.

In conclusion, the Chinese cyberdefense strategies are founded on other Asiatic powers because of the geopolitical and cultural links between those nations woven over time.

An alternative information community, wielding growing saturation power, has been born. Yet from Iran's perspective, this policy is viewed with caution. Regardless of how great a power it is, China's cyber-activity has not yet been able to overcome the Iranian feeling of isolation: China can build virtual bridges through the networks, and protect its allies from cyber-attacks from the outside world, but in today's ever-changing world, Iran still sees itself as an island, relying on a relative degree of isolation to protect itself.

8

Discourse Regarding China: Cyberspace and Cybersecurity

The significant position acquired, in recent years, by discourse analysis in studies conducted in international relations is, to a large extent, attributable to the success of the constructivist paradigm (Nicolas G. Onuf[1], Alexander Wendt[2], Thomas Lindemann[3]), and notably to the techniques of the Copenhagen School (security theories).[4]

Discourse is not a way of learning something about a reality, but rather a way of *producing* reality, rendering

---

Chapter written by Daniel VENTRE

1 Nicholas Greenwood Onuf, *World of Our Making. Rules and Rule in Social Theory and International Relations*, Columbia (SC), University of South Carolina Press, 1989, 341 pages.

2 Alexander Wendt, Anarchy is what States make of it: The Social Construction of Power Politics, *International Organization*, 1992, vol. XLVI, no. 2, pp. 391–425.

3 Thomas Lindemann, *Penser la guerre, l'apport constructiviste*, Paris, L'Harmattan, 2009, 230 pages, p. 31.

4 Thierry Balzacq, Constructivism and Securitization Studies, *in* Myriam Dunn Cavelty, Victor Mauer (*eds.*), *Handbook of Security Studies*, London, Routledge, 504 pages.
[http://graduateinstitute.ch/webdav/site/developpement/shared/developpement/cours/E777/Securitization_Balzacq.pdf].

something a reality.[5] The basic premise of discourse theory runs that the way in which we think and say things reflects the way in which we act in relation to the object of that discourse.[6] Thus, according to this view, there exists no real world untouched by our thoughts, our ideas, and it would be useless to try to distinguish fixed political and social structures, a static reality, independently of our own interpretation of it.[7]

This theory also postulates that language is a form of social power. The social implications of discourse lie in its power to influence, its persuasive nature, its capacity to alter ideas, beliefs and behaviors.[8] Discourse is a social practice

5 Bradley Klein, *Strategic Discourse and its alternatives*, Center on Violence and Human Survival Occasional Paper, New York, January 1987, 24 pages.

6 – Michel Foucault, *Power/Knowledge*, Brighton, UK, Harvester, 1980, 288 pages.

– Michel Foucault, *The Archeology of Knowledge and the Discourse on Language*, London, Tavistock, 1972, 245 pages.

– Stuart Hall (ed.), *Representation: Cultural Representations and Signifying Practices*, London, Sage Publications, 1997, 408 pages.

– Nelson Phillips, Cynthia Hardy, *Discourse Analysis: Investigating Processes of Social Construction*, London, Sage, 2002, 104 pages.

7 Jeremy Moses, *Discourse Analysis and International Politics: Rethinking Relations between the United States and China*, Wuhan, China, International Conference on Political Communication, October 2007 [http://ir.canterbury.ac.nz/bitstream/10092/4989/1/12610075_Wuhan%20Paper.pdf].

8 – Liu Yongtao, Discourse, Meanings and IR Studies: Taking the Rhetoric of "Axis of Evil" As a Case, *CON fines de relaciones internacionales y ciencia política*, January–May 2010, no. 11, pp. 85–107, [http://web2.mty.itesm.mx/temporal/confines/articulos11/YongtaoL.pdf].

– John Langshaw Austin, *Quand dire c'est faire*, Paris, Éditions du Seuil, 1970, 202 pages.

– Pierre Bourdieu, *Ce que parler veut dire : l'économie des échanges linguistiques*, Paris, Fayard, 1982, 239 pages.

which produces the effects of power, i.e. which is aimed at dominating other people.[9]

Discourse analysis, which is a relatively recent method in the field of international relations[10], is commonly used to reveal the established relations between discourse and political practice[11], in order to understand the way in which the textual and social processes are connected, and what the implications of those connections are[12]: how and why the political conditions behind the discourse arise[13]; to reveal the intentions inherent in the discourse[14]; to identify the discursive strategies employed to legitimize[15] political

9 John Langshaw Austin, *How to Do Things with Words*, Oxford, Clarendon Press, 1962, 174 pages.
10 Jennifer Milliken, The Study of Discourse in International Relations: ACritique of Research and Methods, *European Journal of International Relations*, 1999, vol. 5, no. 2, ppp. 225–254.
11 Daniel Sabbagh, *De la rhétorique à la pratique : les tribulations de la politique des États-Unis à l'égard de la Corée du Nord (1994-2002),* Les Études du CERI, no. 89, September 2002 [http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/etude89.pdf].
12 Jim George, *Discourses of Global Politics: ACritical (re) Introduction to International Relations*, Boulder, Lynne Rienner, 1994, 266 pages.
13 Jeremy Moses, *Discourse Analysis and International Politics: Rethinking Relations between the United States and China*, Wuhan, China, International Conference on Political Communication, October 2007
[http://ir.canterbury.ac.nz/bitstream/10092/4989/1/12610075_Wuhan%20Paper.pdf].
14 [http://cadaad.net/files/journal/CADAAD2-2-Reyes-Rodriguez-2008-Hot&Cold_War.pdf].
15 Le pouvoir est un phénomène social qui a constamment besoin d'être légitimé : le langage est le vecteur, le médium de légitimation. Martin Wight*, Power Politics*, Hedley Bull, Carsten Holbraad (eds.), Leicester, Leicester University Press, 1978, 317 pages.

actions (consensus- or consent-seeking; discourse in the service of a particular ideology; etc.).[16]

In this chapter, we examine the changes in the way in which China is viewed (representations, perceptions), by way of analysis of the discourse on the subject of China and its relation with the issues of cyberspace, Cybersecurity and cyberdefense strategies.

The corpora upon which this analysis is founded are as follows:

– for our first section, aimed at identifying the main themes in discourse and research about China (cyberspace, Cybersecurity), we use a very large corpus comprising essentially academic work and resources available on the Internet. We have limited the scope of our observation to resources in English and French;

– for the second section, where the goal is to study the arguments of discourse circulating within the American institutions of power, we draw upon three sources: the annual reports submitted by the Department of Defense to the United States Congress; the projections published by the National Intelligence Council; and the discourse of the successive US Secretaries of Defense. These sources enable us to cover a sufficiently long period of time (DoD annual reports are available for 2002 onwards; the NIC reports for 1997 onwards; and the speeches made by the Secretaries of Defense, online archives begin in 1995), offer the advantage of being available online in their entirety, and reflect the viewpoints of the people in power: the political and military decision-makers, and influential personalities.

16 Ioana Laura Raicu, *Critical Discourse Analysis of the War on Terror – Blairian Discourse and Philosophical Framework*, Recent Advances in Computers, Communications, Applied social science and Mathematics, 2011, pp. 178–182.

To illustrate this discourse, we give many long verbatim quotes, but also show summaries in table form so as to clearly reveal the evolution in terms of themes. The aim is to demonstrate the variables of the available discourses, the relationships between them, and the evolution of those discourses, over the past two decades. This initial analysis could, undoubtedly, later be supplemented by work on the evolution of the discourse conveyed through the media, but also in industrial environments. Finally, an additional project could address the more complex task of reconstructing the path of various ideas (where they first surface; what paths they follow as they are diffused; who has the power to influence). In this chapter, we limit this study of the evolution of ideas to identifying the scenarios which have emerged over the past 20 years.

8.1. Identification of prevailing themes

By way of a state of the art on the work conducted on the subject of China – particularly its relationship to cyberspace – we can see that the discourse on China is organized around relatively few themes, types of discourse, arguments, viewpoints.

8.1.1. *Depictions of the Internet in China*

Many research projects have been conducted on the topic of China's Internet from a historical point of view (when it came about, how its industries have developed, who the designers of the Chinese Net are), from a statistical standpoint (number of users, evolution of uses), but also from a cartographic perspective (how the networks are organized,

how the users and data flows are distributed geographically, etc.).[17]

The sources which can be consulted are many and diverse. Since the late 1990s, such reports have been being published by the Chinese government (White Paper on the Internet in China)[18], the CNNIC (Statistical Report in the Internet Development in China)[19], with regular statistical reports[20] on the evolution of the Internet in the country being published.[21] Many international websites give statistical

17 Gilles Puel, "Géographie des lieux d'accès à Internet. Les conditions de l'accès public et les modèles d'usages dans les grandes villes de Chine*", L'Espace géographique,* 2009, Vol. 38, no. 1, pp. 17–29, [www.cairn.info/revue-espace-geographique-2009-1-page-17.htm].

18 *White Paper on the Internet in China*, 15 June 2010, [http://china.org.cn/government/whitepaper/node_7093508.htm].

19 – CNNIC. *Statistical Report on Internet Development in China*, January 2013, 89 pages, [http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf].

– CNNIC. *Statistical Report on Internet Development in China*, July 2013, 57 pages, [http://www1.cnnic.cn/IDR/ReportDownloads/201310/P020131029430558704972.pdf].

– China Internet Network Information Center (CNNIC), *Statistical Report on the Internet Development in China*, January 2012, [http://www.cnnic.cn/dtygg/dtgg/201201/t20120116_23667.html].

– *Statistical report on Internet Development in China,* 2011, CNNIC, 99 pages, [http://www1.cnnic.cn/uploadfiles/pdf/2011/2/28/153752.pdf].

- *Statistical report on Internet Development in China,* July 2010, CNNIC, 67 pages, [http://www.cnnic.cn/uploadfiles/pdf/2010/8/24/93145.pdf].

– *The 23rd Statistical Survey Report on the Internet Development in China,*[http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/153540.pdf].

– *Statistical Survey Report on the internet development in China,* January 2008, CNNIC, 87 pages, [http://www.cnnic.cn/uploadfiles/pdf/2008/2/29/104126.pdf].

– CNNIC, *The First Statistical Survey Reports on the Internet Development in China,* 1997, 3 pages, [http://www.cnnic.net.cn/download/manual/en-reports/1.pdf].

20 *2008 China Statistical Yearbook*, [http://www.stats.gov.cn/tjsj/ndsj/2008/indexeh.htm].

21 *China Websites Ranking*, [http://main.chinarank.org.cn/statistics/hot_vid.html].

data on the Chinese Internet.[22] Studies are also regularly being produced by researchers, describing China's Internet both from a technical and a general point of view (Liu Dong, 2005[23]; Jane Lael, 2005[24]; Z. Shi, Z. Guo, 2007[25]; Burson-Marsteller, 2011[26]); examining the roles of the actors involved in the Internet (Qiheng Hu, 2007[27]; Zhang Guanqun, Wang Hui, Yang Jiahai, 2009[28]), and the distribution of users (L. He, L. Gui, Q. Le, 2004[29]; Guo Liang, 2005[30]; Guo Liang, 2007[31]).

22 *Sogou User Query Logs*, [http://www.sogou.com/labs/dl/q.html].
23 Liu Dong, *China Internet Overview*, 2005, 13 pages, [http://www.meti.go.jp/report/downloadfiles/gokin11j.pdf].
24 Jane Lael, *Internet in China,* US-China Review, summer 2006, 5 pages, [http://www.uscpfa.org/document/Internet%20in%20China.pdf].
25 Z. Shi, Z. Guo, *Chinese Internet AS-level Topology*, IET Communications. Vol. 1, no.° 2, ppp. 209–214, 2007 .
26 Burson-Marsteller, *State of the Chinese Internet,* March 2011, 57 pages, [http://www.bmchina.com.cn/EN/Documents/Burson-Marsteller_State_of_the_Chinese_Internet_March_2011.pdf].
27 Qiheng Hu, *Internet development in China, Internet society of China and CNNIC*, September 2007, Potsdam, Germany, 30 pages, [http://www.hpi.uni-potsdam.de/fileadmin/hpi/veranstaltungen/china/slides/070919_S1_2_HU_Internet_in_China.pdf].
28 Zhang Guanqun, Wang Hui, Yang Jiahai, *Understanding Web Hosting Utility of Chinese ISPs*, The Network Research Center, Tsinghua University, Tsinghua National Laboratory for Information Science and Technology (TNList), Beijing, China, Lecture Notes in Computer Science Volume 5787, 2009, pp. 11–20, [http://nmgroupp. tsinghua.edu.cn/yang/paper/(54540)Understanding%20Web%20Hosting%20Utility%20of%20Chinese%20ISPs.pdf].
29 He L., Gui L., Le Q., *Spatial-Temporal Analysis of Regional Disparities of Internet in China*. Chinese Geographical Science.14(4), 314-319 (2004).
30 Guo Liang, Surveying Internet usage and impact in five Chinese cities, CASS Internet survey report, Washington, United States, 2005, 144 pages, [http://www.policyarchive.org/handle/10207/bitstreams/15538.pdf].
31 Guo Liang, Surveying Internet usage and impact in seven Chinese cities, CASS Internet survey report, Washington, United States, November 2007, 126 pages, [http://www.policyarchive.org/handle/10207/bitstreams/16013.pdf].

These studies are joined by analyses which focus more specifically on the development of technologies in China:

– the history and evolution of the ICT industry in China (Zhu Gaofeng 2005[32]; Nir Kshetri, 2009[33]; Jiang Zemin, 2010[34]; Xiangning Wu, 2010[35]; George I. Askew, 2010[36]; Guobin Yang, 2012[37]; Michael Pecht, Weifeng Liu[38]; EU Report, 2013[39])

– the impact of China's industrial development on the level of competitiveness of other states, both on a regional level (Zhu W. 2001[40]; Ted Tschang, 2003[41]; Xiangning Wu,

32 Zhu Gaofeng, ICT initiatives in China, China Communications, April 2005, pp. 4–12, [http://www.china-cic.org.cn/english/digital%20library/200504/1.pdf].

33 Nir Kshetri, *The Evolution of the Chinese Online Gaming Industry*, Journal of Technology Management in China, vol.4, no. 2, pp. 158–197, 2009.

34 Jiang Zemin, On the Development of China's Information Technology Industry, 2010, Academic Press, 336 pages.

35 Xiangning Wu, China's ICT Industry and East Asian Regional Production Networks, PhD Thesis, University of Birmingham, 2010, 371 pages, [http://etheses.bham.ac.uk/1150/1/Wu10PhD.pdf].

36 George I. Askew, Steve Rubis, *China Internet Industry – Vast, Unique and Dynamic*, Stifel Nicolaus, November 16, 2010, 48 pages, [http://www.arbaholdings.com/insights/doc/China_Internet_Industry.pdf].

37 Guobin Yang, *A Chinese Internet? History, Practice, and Globalization*, Chinese Journal of Communication, Vol. 5, No. 1, March 2012, 49–54, [http://www.asc.upenn.edu/gyang/CJC_Chinese_Internet.pdf].

38 Michael Pecht, Weifeng Liu, Computers in China, Chapter 3, pp. 47–60, [http://itri2.org/ttec/aemu/report/c3.pdf].

39 *The ICT Market in China*, EU SME Centre, 2013, 18 pages, [http://www.ccilc.pt/sites/default/files/eu_sme_centre_report_the_ict_market_in_china_en.pdf].

40 Zhu W., China Factor in International Division in East Asia of 1990s, China Opening Herald, 06/01/01, p. 15.

41 Ted Tschang, China's Software Industry and its implications for India, OECD Report, February 2003, 37 pages, [http://www.oecd.org/dev/2497604.pdf].

2010[42]) and worldwide, notably analyzing the role of companies such as Huawei, ZTE, Lenovo (Report of the US Congress, 2012[43]; Lucas Solorio, 2014[44]);

– market access conditions applicable to the Chinese Internet (Peter K. Yu, 2001[45]; WilmerHale report, 2006[46]; etc.);

– regulation of industry (Lijun Cao, 2007[47]).

8.1.2. *Impact of cyberspace on Chinese society*

Beyond descriptive, cartographic or statistical (etc.) approaches, the analyses in the existing body of literature focus, in particular, on the social, political, economic and legal transformations caused by the introduction of networking in China: for instance, civilian capability of expression, State surveillance and control of the populace, use of social networks, etc.; to what extent can cyberspace

42 Xiangning Wu, China's ICT Industry and East Asian Regional Production Networks, PhD Thesis, University of Birmingham, 2010, 371 pages, [http://etheses.bham.ac.uk/1150/1/Wu10PhD.pdf].

43 Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, House Permanent Select Committee on Intelligence, October 8, 2012, 60 pages.

44 Lucas Solorio, *China's Evolving IT Capabilities: Cloud Computing, Network Operations and Cyber Espionage*, Nova Science Publishers Inc, 193 pages, March 2014.

45 Peter K. Yu, *Barriers to foreign investment in the Chinese internet industry*, 2001, 5 pages, [http://www.peteryu.com/gigalaw0301.pdf].

46 *A Crackdown on Foreign Involvement in China's Internet Industry?*, September 2006, Wilmer Hale, Briefing series, 4 pages, [http://www.wilmerhale.com/uploadedFiles/WilmerHale_Shared_Content/Files/Editorial/Publication/06_449_China.pdf].

47 Lijun Cao, *A Study on Self-regulatory Initiatives in China's Internet Industry*, 2007, 59 pages, [http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/MScDissertationSeries/Past/Cao_final.pdf].

transform China, on the international stage[48], but also internally (Z. Jonathan; W. Enhai, 2005[49])? What are the instruments (political, legal, etc.) and who are the actors involved in the regulation of the Chinese Internet (Mayer Brown, 2012[50])? Does the Internet have a levelling role in Chinese society (Scott J. Shackelford, 2014[51])?

The political nature of the Internet is noteworthy. Thus, a very great many publications examine the question of the democratization of societies thanks to the new powers granted to individuals by cyberspace (a space for expression, for circumventing censorship, for challenging), and the tension between (cyber) surveillance and sousveillance.

Thus, many works look at the question of democratization, organization of dissidence, the strategies of the Internet users to circumvent the State's surveillance[52], and those of the governments to control the Internet (Philip Sohmen, 2001[53]; Jason P. Abbott, 2001[54]; Michael S.

48 Séverine Arsène, "Chine : Internet, levier de puissance nationale", *Politique étrangère,* 2/ 2012 (Eté), pp. 291–303, [www.cairn.info/revue-politique-etrangere-2012-2-page-291.htm].
49 Jonathan Z., Enhai W., *Diffusion, Use, and Effect of the Internet in China*, Communications of the ACM, Vol. 48, no.°4, pp. 49–53, 2005.
50 Mayer Brown, *New Internet rules in China,* 3 pages, 15 February 2012, [http://www.mayerbrown.com/public_docs/120215_PRC_IPP. pdf].
51 Scott J. Shackelford, "Beyond the new digital divide: analyzing the evolving role of national governments in internet governance and enhancing cybersecurity", *Stanford Journal of International Law*, Vol.5, no. °1, pp. 119–184, 2014.
52 Calum MacLeod, "Chinese create online jokes to vent political frustration", 29 December 2012, *USA Today*, [http://usatoday30. usatoday.com/money/world/2010-12-29-chinainternet29_CV_N.htm].
53 Philip Sohmen, 2001, "Taming the Dragon: China's Efforts to Regulate the Internet", *Stanford Journal of East Asian Affairs*, Spring 2001, Vol.1, pp. 17-26, [http://www.stanford.edu/group/sjeaa/journal1/china1.pdf].
54 Jason PP. Abbott, "Democracy@internet.asia? The challenges of the emancipatory potential of the net: lessons from China and Malaysia", *Third World Quarterly*, vol. 22, n°, pp. 99–114, 2001, [http://courses. essex.ac.uk/gv/gv905/W20%20Readings/internet_china_malaysia.pdf].

Chase, James Mulvenon, 2002[55]; Christopher R. Hughes, 2002[56]; Chin-fu Hung, 2003[57], 2005[58], 2010[59]; OpenNet Initiative reports, 2004[60]; Wei Qi, 2005[61]; Gary D. Rawnsley, 2006[62]; Chunzhi Wang, Benjamin Bates, 2008[63]; Xiaoru

55 Michael S. Chase, James Mulvenon, *Political use of the internet in China*, Chapter 1, 43 pages, dans Michael Case, James Mulvenon, *You've got dissent, Chinese dissident use of the internet and Beijing's counter-strategies*, RAND Corporation, United States, 2002, 132 pages, [http://www.rand.org/pubs/monograph_reports/MR1543.html].

56 Christopher R. Hughes, "Pourquoi Internet ne démocratisera pas la Chine", *Critique internationale* 2/2002 (no. 15), pp. 85–104, [http://www.cairn.info.gate3.inist.fr/revue-critique-internationale-2002-2-page-85.htm#citation].

57 Chin-fu Hung, "Public Discourse and 'Virtual' Political Participation in the PRC: The Impact of the Internet", *Issues & Studies*, Vol. 39, No. 4, December 2003, ppp. 1–38.

58 Chin-fu Hung, The Political Impact of the Internet in the People's Republic of China: A Critical Perspective, Paper presented to the 2005 Annual Meeting of the Taiwan Information Society Association at the Shih Hsin University, Taipei, on 5 June 2005, 38 pages, [http://www.tais.org.tw/doc/2005/2005-8.pdf].

59 Chin-Fu Hung, "The Politics of China's Wei-Quan Movement in the Internet Age", *International Journal of China Studies*, Vol. 1, No. 2, October 2010, pp. 331–349, [http://ics.um.edu.my/images/ics/IJCSV1N2/hung.pdf].

60 – The OpenNet Initiative: Probing Chinese search engine filtering. Bulletin 005, August 2004, [http://www.opennetinitiative.net/bulletins/005/].

– The OpenNet Initiative: Internet Filtering in China in 2004{2005: A Country Study, June 2004, [http://www.opennetinitiative.net/studies/china/ONIChina Country Study.pdf].

61 Wei Qi, Cyberspace and Political Participation in Contemporary China, Lund University, 2005, 52 pages, [http://lupp. lub.lu.se/luur/download?func=downloadFile&recordOId=1326373&fileOId=1326374].

62 Gary D. Rawnsley, The media, Internet and governance in China, China Policy Institute, The University of Nottingham, Discussion paper 12, September 2006, 18 pages,
[http://www.nottingham.ac.uk/cpi/documents/discussion–papers/discussion-paper-12-china-media-internet-governance.pdf].

63 Chunzhi Wang, Benjamin Bates, *Online Public Sphere and Democracy in China*, Paper presented at IAMCR, Stockholm, July 2008, 19 pages, [http://web.cci.utk.edu/~bates/papers/iamcr08-wang-bates-publics.pdf].

Wang, 2009[64]; Ashley Esarey, Xiao Qiang, 2011[65]; Séverine Arsène, 2012[66]; Yiyi Lu, 2013[67]; Jiao Bei, 2013[68]; Loubna Skalli-Hanna, 2013[69]]. The question of censorship and cyber surveillance, which is directly linked to the questions about the democratization of societies, is a crucial one (Jonathan Zittrain, Benjamin Edelman, 2003[70]; James A. Lewis, 2006[71]; Rebecca Mackinnon, 2008[72]; Xiaoru Wang, 2009[73]; Shishir

64 Xiaoru Wang, *Behind the great firewall: the internet and democratization in China,* University of Michigan, United States, 261 pages, 2009, [http://deepblue.lib.umich.edu/bitstream/2027.42/64681/1/wangx_1.pdf].

65 Ashley Esarey, Xiao Qiang, *Digital Communication and Political Change in China*, International Journal of Communication 5 (2011), 298–319, [http://ijoc.org/index.php/ijoc/article/viewFile/688/525].

66 Séverine Arsène, *Protester sur le Web chinois (1994-2011), Le Temps des médias*, 1/ 2012 (no.° 18), pp. 99–110, [www.cairn.info/revue-le-temps-des-medias-2012-1-page-99.htm].

67 Yiyi Lu, *The Extreme Tilt of Chinese Internet Politics*, November 4, 2013, blog The Wall Street Journal, [http://blogs.wsj.com/chinarealtime/2013/11/04/the-extreme-tilt-of-chinese-internet-politics/].

68 Jiao Bei, *How Chinese journalists use microblogging for investigative reporting*, University of Oxford, 2013, 39 pages, [https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/fellows__papers/2012-2013/How_Chinese_journalists_use_Weibo_microblogging_for_investigative_reporting.pdf].

69 Loubna Skalli-Hanna, *Cyber Dissidents: The Potentials and Limitations of Using Social Media for Political Activism,* Washington, American University, Spring 2013, 31 pages, [http://aladinrc.wrlc.org/bitstream/handle/1961/14956/Baumgartner,%20Jackie%20-%20Spring%202013.pdf?sequence=1].

70 Jonathan Zittrain, Benjamin Edelman*, Internet filtering in China*, Harvard Law School Public Law, Research Paper No. 62, Social Science Research Network Electronic Paper Collection, IEEE Internet Computing, March/April 2003, 9 pages, [http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf, [http://ssrn.com/abstract_id=399920].

71 James A. Lewis, *The Architecture of Control: Internet Surveillance in China*, Center for Strategic and International Studies, Washington, United States, July 2006, 8 pages, [http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf].

72 Rebecca Mackinnon, *Cyber Zone, China's online pioneers are pushing the boundaries of free speech*, July 2008, pp. 82–89, [http://www.indexoncensorshipp. org/wp-content/uploads/2008/07/mackinnon_a_308337.pdf].

Nagaraja, 2009[74]; RSF report[75]; Xueyang Xu, Z. Morley Mao and J. Alex Halderman, 2011[76]; Emilie Frenkiel, 2013[77]). Researchers are also posing questions about the reconfiguration of national identities in the Network Age, and the manifestations of nationalism (S. Zhao, 1998[78]; Christopher R. Hughes, 2000[79]; Yu Huang, 2002[80]; Françoise

73 Xiaoru Wang, Behind the great firewall: the internet and democratization in China, 2009, PhD Thesis, University of Michigan, 261 pages, [http://deepblue.lib.umich.edu/bitstream/handle/2027.42/64681/wangx_1.pdf?sequence=1].

74 Shishir Nagaraja, Ross Anderson, *The snooping dragon: social-malware surveillance of the Tibetan movement,* March 2009, technical report n°746, University of Cambridge, United Kingdom, 12 pages, [http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf].

75 *China, journey to the heart of internet censorship*, RSF, October 2007, 17 pages, [http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf].

76 Xueyang Xu, Z. Morley Mao, and J. Alex Halderman, *Internet Censorship in China: Where Does the Filtering Occur?,* N. Spring and G. Riley (*eds.*): PAM 2011, LNCS 6579, ppp. 133–142, 2011., Springer-Verlag Berlin Heidelberg, 10 pages, [http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf].

77 Emilie Frenkiel, *Entre les mailles. L'internet chinois*, pp. 81–94 *in* Emilie Frenkiel, Jean-Louis Rocca (*eds.*), *La Chine en mouvements*, Presses Universitaires de France, 2013, 100 pages.

78 S. Zhao, *A State-led Nationalism: The Patriotic Education Campaign in Post-Tiananmen China*, Communist and Post-Communist Studies, 31(3), pp. 287–302, 1998.

79 Christopher R. Hughes, Nationalism in Chinese Cyberspace, Cambridge Review of International Affairs, 13(2), pp. 195–209, 2000, [http://www.informaworld.com/10.1080/09557570008400309].

80 Yu Huang, *Approaching "Pareto Optimality"? --- A Critical Analysis of Media-Orchestrated Chinese Nationalism*, Intercultural Communication Studies XI, 2, 2002, pp. 69–82, [http://www.uri.edu/iaics/content/2002v11n2/05%20Yu%20Huang.pdf].

Mengin, 2004[81]; Z. Wang, 2008[82]; etc.), which is a potential source of insecurity for other states.[83]

The role of the social media is also essential in these analyses (Louis Yu, 2011[84]; US Congress report, 2011[85]; Edward Tse, Adam Xu, Andrew Cainey, 2012[86]; KPMG report, 2013).[87] The hypothesis usually formulated is that of the *empowerment* of the citizens, for whom the networks represent a forum to express themselves, where there is a relatively reduced degree of control by the authorities over free expression, the capacity to impose a political agenda (Haiqing Yu, 2004[88]; Rebecca Mackinnon, 2010[89]; Qin Guo,

81 Françoise Mengin (ed.), Cyber China: Reshaping National Identities in the Age of Information, CERI Series in International Relations and Political Economy, Palgrave Macmillan, November 2004, 288 pages.
82 Z. Wang, *National Humiliation, History Education, and the Politics of Historical Memory: Patriotic Education Campaign in China*, International Studies Quarterly, 52, pp. 783–806, 2008.
83 W.A. Callahan, *National Insecurities: Humiliation, Salvation, and Chinese Nationalism*, Alternatives, 29, pp. 199–218, 2004.
84 Louis Yu, Sitaram Asur, Bernardo A. Huberman, *What Trends in Chinese Social Media*, The 5th SNA-KDD Workshop'11 (SNA-KDD'11), August 21, 2011, San Diego CA USA, 10 pages, [http://www.hpl.hpp.com/research/scl/papers/chinatrends/china_trends.pdf].
85 *China's censorship of the internet and social media: the human toll and trade impact*, Hearing before the Congressional-executive Commission on China, 17 November 2011, 77 pages, [http://www.cecc.gov/sites/chinacommission.house.gov/files/documents/hearings/2011/CECC%20Hearing%20-%20China's%20Censorship%20of%20the%20Internet%20and%20Social%20Media%20-%2011.17.11.pdf].
86 Edward Tse, Adam Xu, Andrew Cainey, *Impact of social media in China*, Booz&co, 2012, 12 pages, [http://www.strategyand.pwc.com/media/file/Strategyand_Impact-of-Social-Media-in-China_EN.pdf].
87 *Social media in China: Local innovation connecting the country*, KPMG, China 360, April 2013, 5 pages, [https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Newsletters/China-360/Documents/China-360-Issue8-201304-Social-media-in-China-v1.pdf]
88 Haiqing Yu, The power of thumbs: the politics of SMS in urban China, Graduate Journal of Asia-Pacific Studies, 2:2 (2004), 30-43, [http://www.crr.unsw.edu.au/media/File/The_Power_of_Thumbs.pdf].
89 Rebecca Mackinnon, *Networked Authoritarianism in China and Beyond: Implications for global Internet freedom,* Stanford University,

2011[90]; Gary King, Jennifer Pan, Margaret E. Roberts, 2013[91]). The evolution of the Internet in China, its uses, its construction, reflect a "dynamic, changing Chinese society".[92] This upheaval is desired and supported by the State, which has invested heavily in the development of infrastructures, and encourages the development of the information society. In China, like everywhere else, the Web benefits everybody, although it does also expose everybody to new risks: greater openness, fuller communication, more abundant exchanges, freer expression, and greater capacity to watch and control. The revolution in ICTs does not directly lead to democracy. However, it does have political consequences. It impacts on societies' development: the rise in power of the middle classes (who account for the majority of the population of Internet users), the desire for modernization, patriotism, social mobilization, disputes, etc.

It should be pointed out that a number of Chinese authors, or of Chinese descent, have discussed this socio-political aspect of the Internet (Tai Zixue 2006[93]; Zhou Yongming, 2006[94]; Xu Wu 2007[95]; Yongnian Zheng 2007[96];

paper presented at Liberation Technology in Authoritarian Regimes, 11-12 October 2010, 31 pages, [http://iis-db.stanford.edu/evnts/6349/MacKinnon_Libtech.pdf].

90 Qin Guo, *Internet and political participation in China*, Masaryk University Journal of Law and Technology, vol.5, no. 1, 2011, pp. 83–103, [http://mujlt.law.muni.cz/storage/1327951326_sb_08-guo.pdf].

91 Gary King, Jennifer Pan, Margaret E. Roberts, *How Censorship in China Allows Government Criticism but Silences Collective Expression*, American Political Science Review, May 2013, 18 pages, [http://gking.harvard.edu/files/gking/files/censored.pdf].

92 Emilie Frenkiel, *Entre les mailles. L'internet chinois*, in Emilie Frenkiel, Jean-Louis Rocca (*eds.*), *La Chine en mouvements*, Presses Universitaires de France, 2013, p. 81.

93 Tai Zixue, The Internet in China: Cyberspace And Civil Society, 2006.

94 Zhou Yongming, Historicizing Online Politics: Telegraphy, the Internet, and Political Participation in China, 2006, 304 pages, Stanford University Press.

95 Xu Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*, Lexington Books, United States, 2007, 280 pages.

Rebecca Fannin 2008[97]; Sherman So and J. Christopher Westland 2009[98]; Tiebing Xu, 2009[99]; Hong Xue, 2010[100]; Yun Zhao2011[101]; Wang Jun 2011[102]; Guobin Yang 2011[103]; Rodney Wai-chi Chu, Leopoldina Fortunati, Pui-Lam Law, Shanhua Yang, 2012[104]; Guosong Shao, 2012[105]).

8.1.3. *The Chinese cyber threat*

The "Chinese cyber threat" plays an important part in the considerations about China's evolution and the relations it can have with the rest of the world.[106] China's practices in cyberspace, its policies and strategies for Cybersecurity and

96 Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China,* Stanford University Press, United States, November 2007, 272 pages.
97 Rebecca Fannin, *Silicon Dragon: How China Is Winning the Tech Race*, McGraw-Hill, January 2008, 300 pages.
98 Sherman So, J. Christopher Westland, *Red Wired: China's Internet Revolution*, Marshall Cavendish Limited, November 2009, 256 pages.
99 Tiebing Xu, L'émergence des opinions parallèles, *Hermès, La Revue* 3/ 2009 (no. 55), pp. 80–82, [www.cairn.info/revue-hermes-la-revue-2009-3-page-80.htm].
100 Hong Xue, Cyber Law in China, 2010.
101 Yun Zhao, Cyber Law in Hong Kong, 2011.
102 Wang Jun, *Cyber Nationalism and China's Foreign Affairs*, China Social Sciences Press, January 2011, 299 pages.
103 Guobin Yang, *The Power of the Internet in China: Citizen Activism Online*, Columbia University Press, 320 pages, 2011.
104 Rodney Wai-chi Chu, Leopoldina Fortunati, Pui-Lam Law, Shanhua Yang, Mobile Communication and Greater China, Routledge Research on Social Work, Social Policy and Social Development in Greater China, 2012.
105 Guosong Shao, Internet law in China, Chandos Asian Studies, 2012.
106 David Hanel, *Chinese Cybercrime - A Threat to the Occident? The Impact of Chinese Cybercrime on EU –China Relation*s, University of Twente, Netherlands, June 2013, 45 pages, [http:// essay.utwente.nl/63300/1/Bachelor_Paper_Final_Version_d.hanel_s1062336.pdf].

cyberdefense are even often defined as being indicative of China's true ambitions on the international stage.

Also, many observers view the cyber threat as being only one facet of the threat constituted by China, which is engaged in a processof growth, but whose unpredictable evolution presents cause for concern.

These issues (cyber threat, Cybersecurity, cyberdefense, cyber-policy and strategies) thus fit into the more global discourse about the Chinese threat. They are the topic of specific publications, which emerged in the United States in the 1990sand have since been widely disseminated the world over.

The topic of cyber threat is jointed around a number of variables:

– the identity of the actors:

- State services: the army, the intelligence services, etc.,[107]

- non-State actors: hackers[108], hacktivists, cybercrime[109], cyber nationalism (on the forms of expression of Chinese cyber nationalism in opposition to Japanese nationalism),[110]

107 Tobias Feakin, *Enter the Cyber Dragon, Understanding Chinese intelligence agencies cyber capabilities,* Special Report, ASPI, Australia, June 2013, 12 pages, [https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf].

108 – Victor Benjamin, Hsinchun Chen, Securing cyberspace: identifying key actors in hacker communities, 2013, 6 pages, [http://web.elastic.org/~fche/mirrors/www.jya.com/2013/03/key-hackers.pdf].

– Jack Linchuan Qiu, *Chinese Hackerism in Retrospect: The Legend of a New Revolutionary Army*, 14 pages, [http://ncsi-net.ncsi.iisc.ernet.in/cyberspace/societal-issues/Qiu1.pdf].

- the rising Chinese industry

– policies and strategies

- political will,

- justifying means and methods by service to the objective of economic, industrial, technological (etc.) catchup,

- military development strategy, creation of a cybernetic strike force,

- a lack of determination to really fight cybercrime,

- differing views (and values) with the West over the governance of cyberspace,

- the absence of China's consensus over the application of the law on armed conflicts and international humanitarian laws in cyberspace;

– practices:

- cyber-attacks (and the difficulty in evaluating the extent of the phenomenon[111]),

---

109 – *Risk Briefing Paper: China & Cyber Crime,* KCS Country Risk & Threat Advisory, 20 December 2011, 9 pages, [http://www.kcsgroupp.com/wp-content/uploads/2012/01/KCS_China.pdf].
– Council of Europe, *China, Cybercrime Legislation, Country Profile*, 28 March 2008, 39 pages, [http://www.cyberlawdb.com/gcld/wp-content/uploads/2010/04/china.pdf].
– Man Qi, Yongquan Wang, Rongsheng Xu, *Fighting cybercrime: legislation in China*, Int. J. Electronic Security and Digital Forensics, Vol. 2, No. 2, 2009, pp. 219–227, [http://inderscience.metapress.com/content/a67161603x6x8011/].
110 Flora Yufen Wang, *Riding the Tiger, Chinese Cyber Nationalism and the Sino-Japanese Relationship*, Stanford University, Thesis, 31 May 2013, 146 pages, [http://iis-db.stanford.edu/docs/785/Wang_Flora_Thesis_Final.pdf]
111 – Michael Riley, John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg, Dec 14, 2011, [http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html].

- underground crime[112],

- industrial, political and military espionage practices[113],

- an industrial strategy with in the State intelligence service (the company Huawei is described as representing a danger for the security of other states in the markets to which it has access.[114]The company can be described as the industrial branch of the intelligence services of the Chinese military),

- practices described as aggressive (cyber-attacks in all directions),

- the combination of State-sanctioned and non-State action (hacktivism, cybercrime, etc., from the late 1990s).

The discourse about international insecurity, rooted in the worrying evolution of Chinese State- and non-State capacities and practices in cyberspace, dates from the end of

– Robert Lai, Syed (Shawon) Rahman, Analytic of China Cyber-Attack, The International Journal of Multimedia & Its Applications (IJMA), Vol.4, No.3, June 2012, pp. 37-56, [http://airccse.org/journal/jma/4312ijma04.pdf].

112 – Zhuge Jianwei, Gu Liang, Duan Haixin, *Investigating China's Online Underground Economy*, IGCC, University of California, July 2012, 54 pages, [http://igcc.ucsd.edu/assets/001/503677.pdf].

– Lion Gu, *The Mobile Cybercriminal Underground Market in China*, Cyber Criminal Underground economy Serie S, A Trend Micro Research Paper, 2014, 17 pages, [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf].

113 James A. Lewis, *Computer Espionage, Titan Rain and China,* Center for Strategic and International Studies – Technology and Public Policy Program, December 2005, 2 pages, [http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf].

114 Mike Rogers, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Congress, October 8, 2012, 52 pages, [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf].

the 1990s and the start of the 2000s (T. Yoshihara, 2001[115]; Peter Hays Gries[116], whose study relates to the expression of Chinese nationalism following the bombing of the Chinese Embassy in Belgrade in 1999). Since then, a copious body of literature has been produced on this subject, and the overview given here is not, by any stretch of the imagination, intended to be exhaustive. Let us simply cite the works of John Tkacik, 2008[117]; Jayadeva Ranade, 2010[118]; Derek Scissors, Steven Bucci, 2012.[119]

In the discourse in the media worldwide about Cybersecurity, the Chinese hacker has become an imposing and unavoidable figure. However, s/he is absent from the academic reference works on the sociology of hackers from the late 1990s[120], or even more recent works[121], on the

115 T. Yoshihara, Chinese Information Warfare a Phantom Menace or Emerging Threat? Carlisle, Strategic Studies Institute, U.S. Army War College, 2001.

116 Peter Hays Gries, *Tears of rage: Chinese nationalist reactions to the Belgrade Embassy bombing*, The China Journal, n°46, July 2001, pp. 25-43, [http://www.ou.edu/uschina/gries/articles/texts/TearsofRage.pdf].

117 John Tkacik, *Trojan Dragon: China's Cyber Threat*, 8 February 2008. [http://www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat].

118 Jayadeva Ranade, *China and the latent cyber threat*, Centre for Air Power Studies, New Delhi, 1 March 2010, 5 pages, [http://capsindia.org/files/documents/ISSUE-BRIEF_22_CHINA-AND-THE – LATENT-CYBER-THREAT_01-March-2010.pdf].

119 Derek Scissors, Steven Bucci, *China Cyber Threat: Huawei and American Policy Toward Chinese Companies*, The Heritage Foundation, Issue Brief, Washington, October 23, 2012, n°3761, 3 pages, [http://thf_media.s3.amazonaws.com/2012/pdf/ib3761.pdf].

120 Tim Jordan, Paul Taylor, *A sociology of hackers*, Blackwell Publishers, pp. 757–780, 1998, [http://cj-resources.com/CJ_Crim_Theory_pdfs/A%20sociology%20of%20hackers%20-%20Jordan%20et%20al%201998.pdf].

121 Thomas J. Holt, Deborah Strumsky, Olga Smirnova, Max Kilger, *Examining the Social Networks of Malware Writers and Hackers*, International Journal of Cyber Criminology, Vol 6 Issue 1 January – June 2012, pp. 891–903, [http://www.cybercrimejournal.com/holtetal2012janijcc.pdf].

psychology of hackers.[122] China is believed to be targeting cyber-attacks in all directions, without imposing any limitations at all on that activity (testing what it is possible to do, and attacking anything and everything that is exposed).[123] Chinese hacking could have a significant impact on trade law and human rights.[124] The phenomenon is so widespread that 2008 could, in fact, be dubbed the "*Year of the Chinese hacker*".[125]

The literature about Chinese hackers mentions:

– non-State-sanctioned cyber-espionage[126];

122 Christian S. Fötinger, Wolfgang Ziegler, Understanding a hacker's mind – A psychological insight into the hijacking of identities, Danube-University Krems, Austria, 48 pages, [http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf].

123 Josh Rogin, *Cyber Officials: Chinese Hackers Attack 'Anything and Everything'*, FCW.com, February 13, 2007, [https://www.grc.com/sn/files/fcw_on_%20cyber_warefare.pdf].

124 *Chinese Hacking: impact on human rights and commercial rule of law*, Hearing before the Congressional-executive Commission on China, 113th Congress, 1st Session, USA, June 25, 2013, 58 pages, [http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg81855/pdf/CHRG-113hhrg81855.pdf].

125 Formule qui aurait été utilisée par des experts en sécurité de la société Arbor Networks. Cited in: Scott Henderson, *Beijing's Rising Hacker Stars… How Does Mother China React?*, IO Sphere, Fall 2008, pp. 25-30.

126 – Scott Henderson, *Beijing's Rising Hacker Stars… How Does Mother China React?*, IO Sphere, Fall 2008, pp. 25–30, [http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf].
– Zhang Jianwen, The current situation of cybercrimes in China, International Centre for Criminal Law Reform and Criminal Justice Policy, Vancouver, Canada, November 2006, [http://www.icclr.law.ubc.ca/china_ccprcp/files/Presentations%20and%20Publications/47%20The%20Current%20Situation%20of%20Cybercrime%20in%20China_English.pdf]

– the significance of cybercrime (Michael Yip[127]; Zhuge Jianwei, Gu Liang, and DuanHaixin[128]; Aidong Xu, Yan Gong, Yongquan Wang, Nayan Ai[129]), as a phenomenon in juvenile crimes[130]; in international relations (Lennon Yao-Chung Chang writes about the prevention of cybercrime, specifically in the context of the relations between continental China and Taiwan[131]), or indeed the threat to the West (David Hanel, 2013[132]); certain authors attribute the dynamism of this threat to the permissive attitude of the Chinese State;

127 Michael Yip, *An investigation into Chinese cybercrime and the underground economy in comparison with the West*, 2011, [http://journal.webscience.org/411/1/yipp. pdf].

128 Zhuge Jianwei, Gu Liang, DuanHaixin, *Investigating China's Online Underground Economy*, University of California, IGCC, July 2012, 54 pages, [http://www-igcc.ucsd.edu/assets/001/503677.pdf].

129 Aidong Xu, Yan Gong, Yongquan Wang, Nayan Ai, *On Different Categories of Cybercrime in China*, Forensics in Telecommunications, Information, and Multimedia, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 56, 2011, pp. 277-281.

130 Yao Chung Lennon Chang, Sing Wing Dennis Wong, *Cyber-crime and cyber-deviance among adolescents in Hong-Kong*, City University of Hong Kong, HKFYG Youth Crime Prevention Centre, July 2013, 91 pages, [http://ycpc.hkfyg.org.hk/files/youthlaw/download/201307-web-cyber-crime_and_cyber-deviance_among_adolescents_in_hong_kong.pdf].

131 Lennon Yao-Chung Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Edward Elgar, January 2013, 272 pages.

132 David Hanel, *Chinese Cybercrime – A Threat to the Occident? The Impact of Chinese Cybercrime on EU – China Relation*s, University of Twente, Netherlands, June 2013, 45 pages, [http://essay.utwente.nl/63300/1/Bachelor_Paper_Final_Version_d.hanel_s1062336.pdf].

– military-based operations (intelligence units[133] stealing intellectual property on a worldwide scale[134]);

– the intervention of patriotic/nationalistic hackers, hacktivists (hackers whose motives are political), who have been besieging the networks for nearly 20 years, and whose practices are specifically examined in works such as those of Michael Yip and Craig Webber, who call them "cyber-warriors"[135]; Alexandra Samuel[136], who compares them to cyber activists, one of whose main objectives is to circumvent the State's cyber control mechanisms; and Sheo Nandan Pandey[137], who seeks to identify the Chinese characteristics of this hacktivism.

133 Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 76 pages, February 2013, [http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf].

134 James Lewis, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, Testimony, Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2013, 10 pages, [http://csis.org/files/attachments/ts130709_lewis.pdf].

135 Michael Yip, Craig Webber, *Hacktivism: a Theoretical and Empirical Exploration of China's Cyber Warriors*, 2011, WebSci '11, June 14-17, 2011, Koblenz, Germany, 8 pages, [http://www.websci11.org/fileadmin/websci/Papers/59_paper.pdf].

136 Alexandra Samuel, *Hacktivism and the Future of Political Participation*, Chapter I, 35 pages, 2006, [http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-chapter1.pdf].

137 Sheo Nandan Pandey, Hacktivism of Chinese Characteristics and the Google Inc. Cyber-Attack Episode, ISPSW Institute for Strategic, Political, Security and Economic Consultancy, 2010, 8 pages, [http://mercury.ethz.ch/serviceengine/Files/ISN/113440/ipublicationdocument_singledocument/2533e975-eb94-4b60-97c3-8ac96ee73ddd/en/Hacktivism_Pandey_Mar10.pdf].

Figure 8.1. *Hacktivism: defacement of a Website, signed by the group Honker Union of China. The content of the slogan displays the desire to defend the interests of the Chinese nation*[138]

Figure 8.2. *Screenshot of the Website http://www.ssol.com/ defaced by China Honkers*[139]

138 Image source: [http://www.wyxuan.com/pic/hacker/22.jpg]. Placed online in 2011. Downloaded on 20 March 2014.

139 Other screenshots from websites defaced by Chinese hacktivists are available at: [http://cache.baiducontent.com/c?m=9d78d513d9d706ef06e2ce384b54c0676a499d33628a85027fa3d31fcf240c1d506694ea7a7d0d4589963c301caa4b5ceaf7367235083db69bce8d4ddabf972e2d&p=8b2a975490934ead0cf1c52a4d&newp=8b2a970786cc43fe02b3dd3c1b53d8304a02c70e3f95&user=baidu].

8.1.4. *The Chinese army: its practices, capabilities and strategies*

The Chinese army, its strategies, its developments in terms of capacity, its manifest interest in information warfare, mastery of information space (and cyberspace), and the increasing use of computerization in the forces (or more specifically the notion of *informationization*, which covers the computerization of weapons systems but also the integration of operations in cyberspace), modernization of the forces as part of the revolution in military affairs[140], are the focus of a not-insignificant portion of literary production, mainly in the form of official reports produced by or for the American administration.

These works may relate to the impact of China's cyber-policies on international relations.

Amongst the numerous English-language publications on these subjects, we can cite the most significant as being: the work of James Mulvenon (1999)[141], Toshi Yoshihara (2001)[142], Nina Hachigan (2001)[143], Timothy L. Thomas

140 Arthur S. Ding, *China's Revolution in Military Affairs: An Uphill Endeavour*, Security Challenges, vol. 4, no. 4 (Summer 2008), pp. 81–99, [http://securitychallenges.org.au/ArticlePDFs/vol4no4Ding.pdf].

141 James Mulvenon, *The PLA and Information Warfare*, in James Mulvenon, Richard H. Yang (eds.), *The People's Liberation Army in the Information Age*, 297 pages, 1999, RAND Corporation, Washington, United States, pp. 175-186, Actes de la conférence tenue à San Diego, Californie, 9-12 July 1998, [http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf; [http://www.rand.org/pubs/conf_proceedings/CF145.html].

142 Toshi Yoshihara, *Chinese Information Warfare: a phantom menace or emerging threat?* Strategic Studies Institute, November 2001, 41 pages, [http://www.au.af.mil/au/awc/awcgate/ssi/chininfo.pdf].

143 Nina Hachigan, *China's Cyber-Strategy*, Foreign Affairs 80, no. 2, 2001, pp. 118–133.

(2001[144], 2004[145], 2006[146], 2007[147], 2009[148]), Ken Dunham and Jim Melnick (2006)[149], Brian Mazanec (2008)[150], Kevin Coleman (2008)[151], Ron Deibert and Rafal Rohozinski (2009)[152], Bryan Krekel and George Bakos[153], Jeffrey Carr

144 Timothy L. Thomas, *The Internet in China: Civilian and Military Uses, Information & Security, An International Journal,* Volume 7, 2001, pp. 159–173, [http://library.uoregon.edu/ec/e-asia/read/netuse.pdf].

145 Timothy L. Thomas, *Dragon Bytes: Chinese information war theory and practice,* Foreign Military Studies Office, 2004, 168 pages, United States; [http://www.ists.dartmouth.edu/events/abstract-TimThomas.html].

146 Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations,* Foreign Military Studies Office, 334 pages, United States.

147 Timothy L. Thomas, *Decoding The Virtual Dragon – Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy – The Art Of War And IW,* Foreign Military Studies Office (FMSO), United States, 2007.

148 Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations,* Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, United States, 2009, 298 pages.

149 Ken Dunham, Jim Melnick, *'Wicked Rose' and the NCPH Hacking Group*, VeriSign iDefense, 2006.

150 Brian Mazanec, *Cyberwarfare as an Element of PRC National Power and its Implications for U.S. National Security,* Brian Mazanec Pub., Amazon Digital Services, 113 pages, December 2008.

151 K. Coleman, Defense Tech: China's Cyber Forces, 8 May 2008, Defensetech.org, [http://defensetech.org/2008/05/08/chinas-cyber-forces/].

152 Ron Deibert, Rafal Rohozinski, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Sec Dev Group & University of Toronto, Munk Centre for International Studies, 29 March 2009, Canada, 53 pages, [http://www.nartv.org/mirror/ghostnet.pdf].

153 – Bryan Krekel, George Bakos, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corp, prepared for the US-China Economic and Security Review Commission, 9 October 2009, 61 pages, United States, [http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf].

– Bryan Krekel, Patton Adams, George Bakos, *Occupying the information high-ground; Chinese capabilities for computer network operations and cyber-espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, 7 March 2012, 136 pages, United States, [http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf].

(2009)[154], Gurmeet Kanwal (2009)[155], R. A. Clarke and R. Knake (2010)[156], Elisabette M. Marvel (2010)[157], Martin Libicki (2011)[158], Dmitri Alperovitch (2011)[159], Venusto Abellera (2011)[160], C. Paschal Eze (2011)[161], Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao (2011)[162], Li Yan (2012)[163],

154 Jeffrey Carr, *Inside Cyber Warfare: mapping the cyber underworld*, O'Reilly Media, United States, December 2009, 240 pages.

155 Gurmeet Kanwal, *China's emerging cyberwar doctrine, Journal of Defense Studies*, pp. 14–22, vol.3, no. °3, July 2009, [http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf].

156 R. A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* Ecco Publisher, United States, April 2010, 320 pages.

157 Elisabette M. Marvel, *China's Cyberwarfare Capability*, 105 pages, Nova Science Pub Inc, 31 October 2010.

158 Martin Libicki, *Chinese use if cyberwar as an anti-access strategy*, Testimony presented to the U.S. China Economic and Security Review Commission, 27 January 2011, Publication Rand Corporation, 6 pages, [http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT355.pdf].

159 Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, 2011, [http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf].

160 Venusto Abellera, *Exploring China's Use of Known Cyber Capabilities in the Intrusions of United States Public Sector Networks*, ProQuest, UMI Dissertation Publishing, 124 pages, September 2011.

161 C. Paschal Eze, *Cyber Coexistence Code: Whither U.S.-China Cyber Cold War?,* Global Mark Makers, 29 pages, October 2011.

162 Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao*, The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,* Project 2049, 11 November 2011, 32 pages, [http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf].

163 Li Yan, *The Global Commons and the Reconstruction of Sino–U.S. Military Relations*, Asia paper, March 2012, 35 pages, [http://www.isdpp.eu/images/stories/isdp-main-pdf/2012_li-yan_the-global-commons.pdf].

William T. Hagestad (2012)[164], Dennis F. Poindexter (2013), Larry M. Wortzel (2014).[165]

It would be remiss to neglect to mention the official reports painting China as a potential threat because of the development of its military capabilities. In seeking to uncover the view of the Americans, we can exploit the following resources:

– the annual reports[166] of the US Defense Department relating to the development of Chinese military power, which always give a substantial amount of attention to the issues of information warfare and cyberspace (reports published since 2000);

– the reports to Congress given by the *U.S.-China Economic and Security Review Commission* (published annually since July 2002);[167]

– the discourse from the *CIA* (online archives covering 1995 to present);[168]

– the discourse from the *NSA* and hearings before Congress (since 2000);[169]

164 William T. Hagestad, *21st Century Chinese Cyber Warfare,* IT Governance Publishing, Cambridge, United Kingdom, 314 pages, 1° March 2012.

165 Larry M. Wortzel, *China's Military Modernization and Cyber Activities,* Strategic Studies Quarterly, Pennyhill Press, March 2014, 22 pages, [http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/wortzel.pdf].

166 Department of Defense, United States, *Annual Report to Congress. Military Power of the People's Republic of China,* 2000 and subsequent.

167 Law from 2000.Last report dates from November 2012.

168 [https://www.cia.gov/news-information/speeches-testimony/1995/index.html].

169 [http://www.nsa.gov/public_info/speeches_testimonies/].

– the discourse from the *Department of Homeland Security* (available from 2010 onwards);[170]

– the analyses and discourse of the US Congress (for instance, see Frank Wolf's site);[171]

– works of the *USCC Research Staff* (2011)[172], from the *United States House of Representatives*[173] through the productions of its various committees (e.g. this reportfrom 2011 on Chinese cyber-attacks)[174], the *Office of the National Counterintelligence Executive* (2011)[175] or the US *National Intelligence Estimate* (classified report, 2013);[176]

170 [http://www.dhs.gov/news-releases/speeches].

171 Frank Wolf, *Change needed in addressing cyber threat*, Congressman, 10th District of Virginia, October 22, 2013, [http://wolf.house.gov/media-center/press-releases/wolf-change-needed-in-addressing-cyber-threat#.U234Ovl_vX4].

172 USCC Research Staff, *The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector*, 104 pages, January 2011, Create Space Independent Publishing Platform.

173 [http://search.house.gov/htbin/search].

174 United States House of Representatives, *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*, United States, 30 June 2011, 91 pages, Kindle Edition available at: [http://www.amazon.com/Communist-Cyber-Attacks-Cyber-Espionage-Technology-ebook/dp/B005966LG2/ref=sr_1_7?s=books&ie=UTF8&qid=1364229259&sr=1-7&keywords=cyber+china].

175 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, October 2011, 31 pages, United States, [http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf].

176 The report is believed to confirm that China is the main cyber threat facing America. The existence of the document is mentioned in various press articles – e.g. Stacy Curtin, China is America's #1 Cyber Threat: U.S. Govt. Report, 11 February 2013, [http://finance.yahoo.com/blogs/daily-ticker/china-america-1-cyber-threat-u-govt-report-150621517.html].

– a report from the *Committee on Homeland Security, House of Representatives*[177], including China in a specific group of actors posing a cyber threat (China, Russia and Iran).

Reports from Cybersecurity companies contribute to this discourse about the actions of the Chinese army in cyberspace. The report most recently released in the media was produced by the American company Mandiant, in 2013.

8.1.5. *Espionage*

The question of cyber-espionage, which is an issue of strategic importance[178], is cross-cutting, and therefore is included in works on cybercrime, cyber-attacks and State practices.

Whilst it clearly offers an advantage to infiltrate the computer systems of major enterprises, State services, armed forces, etc., the same actions directed at more modest actors raise questions: "*Google Inc. (GOOG) and Intel Corp. (INTC) were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining* […] *The hackers' interest in companies as small as Salt Lake City-based iBahn illustrates the breadth of China's spying against firms in the U.S. and elsewhere. […] "They are stealing everything that isn't bolted down, and it's getting exponentially worse," said Representative Mike Rogers, a*

177 Committee on Homeland Security House of Representatives, *Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure*, 50 pages, January 2014.

178 Magnus Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, Journal of Strategic Security, Volume IV Issue 2 2011, pp. 1–24, [http://cryptocomb.org/Espionage%20Meets%20Strategic%20Deterrence.pdf].

Michigan Republican who is chairman of the Permanent Select Committee on Intelligence".[179] This "no-holds-barred" strike is perhaps attributable to the voracious appetite of China, which is determined to make up lost ground (in terms of knowledge, technologies, all kinds of expertise) and, as quickly as possible, turn itself into a competitor or a credible alternative to American power. Scott Borg, Director of the US Cyber Consequences Unit, denounced what he believes "*…may be the biggest transfer of wealth in a short period of time that the world has ever seen*."[180]

According to the US authorities, it is in this respect that Chinese espionage is radically different from that of the United States: the American cyber spies target the secrets of foreign governments, military secrets, and fight against terrorism. American cyber-espionage, it seems, is acceptable because it fits into the context of an acceptable norm – that of the power game on the international scene – and is only for defensive purposes (to protect the country against future threats). Chinese espionage goes beyond the bounds of the norm, attacking illegitimate targets, and having offensive objectives. With this discourse, the United States refuses to assume the role of the villain, which they place on the shoulders of China, Russia and Iran.

The threat constituted by Chinese cyber-espionage is apparently different from the cybercrime which takes place in the rest of the world. It is held to be a major threat, as "*China's economic espionage activities against the United States are greater than the economic espionage activities are*

179 Michael Riley, John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg, Dec. 14, 2011, [http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html].

180 Cited in Michael Riley, John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg, Dec. 14, 2011, [http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html].

of all other countries combined."[181] Many official reports are devoted to defining that threat.[182]

However, the author of that assessment, who feels the need to avoid any exaggerated statements *("Many discussions of Cybersecurity invariably involve exaggeration. The source of this exaggeration is often a lack of specificity in precisely assessing intent, capabilities, and effect"),* tempers his judgment: "*The effect, however, is not one of clear-cut benefit to China. The strategic implications of this theft are difficult to assess. Some call it the greatest transfer of wealth in history; others call it a rounding error for an economy as big as that of the U.S. Neither characterization is correct*". However, China's espionage activities are singled out*: "What is unacceptable is espionage for purely commercial purposes […] Where China's espionage efforts differ significantly from international practice is in the rampant economic espionage carried out by Chinese government entities, including the PLA".*

Hence, returning to the example of the attack on Google a few years ago (2009-2010), James Lewis defines the acceptable limit: provided China's intelligence services are attacking systems for subjects in the areas of security and national defense, it is acceptable; when those same espionage operations are used to steal industrial secrets, it becomes scandalous. The disagreement between China and the rest of the world appears to lie in this difference of opinion, the lack of sharing of international norms that are tacitly accepted by the actors within this international community.

---

181 James Lewis, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, Testimony, Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2013, page 4.

182 *Occupying the information High Ground: Chinese capabilities for Computer Network Operations and Cyber Espionage*, Report prepared for the U.S.- China Economic and Security Review Commission by Northrop Grumman Corp. , March 7, 2012, 136 pages.

Other stances seem to demonstrate China's incompatibility with the "norms" of the international community: at the ITU conference, China proposed rules which were different to those accepted by the West. It marginalizes itself by way of its practices, its choices, its way of acting and thinking. Yet the problem of the background discord does not only involve China, because from the Western point of view, there are many states which do not conform to the norm, and the motives are numerous, especially in terms of respecting the fundamental values defined by the West as universal standards.

The West's position, or at least that of the United States, seems firmly rooted. The solution proposed by James Lewis in his discussion of how to deal with the issue of Chinese cyber-espionage is essentially to attempt to change China's behavior. In Lewis' eyes, China's "*economic espionage provides a technology boost, but puts bilateral relations with the U.S. at risk and hampers China's ability to create indigenous innovation*".[183] There are significant limitations on the pressure which the USA can exert on China: "*This is not a new Cold War. We cannot have a Cold War with one of our largest trade partners*".[184]

Published in February 2013, the report *APT1: Exposing One of China's Cyber-espionage Units*[185] claims to provide proof of the existence of Chinese military groups specializing in cyber-espionage operations, specifically targeting the United States. The survey, which examines 150 incidents

183 James Lewis, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, Testimony, Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2013, page 7.
184 James Lewis, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, Testimony, Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2013, page 7.
185 Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 76 pages, February 2013, [http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf].

observed over a period of 7 years, was able to reconstruct the profile of Unit 61398, attached to the 2nd bureau of the PLA, 3rd Department, located near to Shanghai. Besides this group, the authors of the report also claim to be observing dozens of others distributed throughout the world – around twenty of them in China.

All of the literature produced about Chinese cyberwarfare and information warfare capabilities has, since the 1990s, been painting the picture of an aggressive, fearsome nation, possessed of inexhaustible capacities (because when it is not a question of the threats represented by State actors themselves, it is a question of cybercriminals or indeed millions of citizens turned nationalistic hackers, constituting as many threats for the rest of the planet, in view of their skills and their motives); a nation whose defense strategies are unclear[186], whose current approach of attacks carried out in information space is rooted in secular warrior practice (Sun Tzu's *The Art of War*, Chairman Mao's irregular warfare). This portrait is based on the existence of forces of techno-warriors set up during the Cold War[187], and expresses China's determination to establish itself as an alternative to America's hegemonic power, thus upsetting the international order established at the end of the Cold War. Faced with this situation, America and the whole of the industrialized world

186 – Richard Halloran, *The Opacity of China's Military*, The Washington Times (Washington, DC), 10 March 2009.
– Kristopher Harrison, *Why China's economic opacity is a serious problem*, Foreign Policy, 10 July 2012, [http://shadow.foreignpolicy.com/posts/2012/07/10/why_chinas_economic_opacity_is_a_serious_problem].
– Kerry B. Collison, *Opacity the heart of China's PLA strategy,* 10 June 2010, [http://kerrycollison.blogspot.fr/2010/06/opacity-heart-of-chinas-pla-strategy.html].
– Office of the Secretary of Defense, *Annual Report to Congress, Military Power of the People's Republic of China,* 2008, United States, 66 pages, p. I, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].
187 Evan Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age*, Stanford University Press, Stanford, United States, April 2003, 360 pages.

is in a vulnerable and inferior position (R. Clarke[188]; Joel Brenner[189]) because of their dependency on cyberspace, the number of potential enemies and the motives held by those foes, and seems to have no option but to prepare for confrontation by trying to make up their lost ground in terms of capabilities, both defensive and offensive.[190] An alarmist discourse, rooted in the predictions made during the 1990s of a Cyber Pearl Harbor and other forms of cybernetic chaos, has taken hold amongst the political classes (for example, the Republican US Senator Mike Rogers declares that the United States is losing the cyberwar against China).[191]

It should also be noted that the subject of the Chinese cyber threat is often discussed by military or ex-military personnel: Timothy L. Thomas[192], Scott J. Henderson[193], Rich Barger[194], Mark. A. Stokes[195] and William T. Hagestad[196] are

188 R. A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* Ecco Publisher, United States, April 2010, 320 pages.

189 Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, The Penguin Press HC, United States, September 2011, 320 pages, J. Brenner was a legal counsellor on cybersecurity for the NSA (United States).

190 Defense Science Board, *Resilient Military Systems and the advanced cyber threat*, Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington DC, 20301-3140, United States, January 2013, 146 pages, [http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf].

191 Mike Rogers, *America is losing the cyber war vs. China*, 8 February 2013, [http://www.detroitnews.com/article/20130208/OPINION01/302080328/1007/OPINION/Rogers-America-losing-cyber-war-vs-China].

192 Lieutenant Colonel Timothy L. Thomas was an an analyst in the FMSO (Foreign Military Studies Office), at Fort Leavenworth (Kansas, United States), Director of USARI, Soviet Studies – United States Army Russian Institute, at Garmischin Germany.

193 Scott J. Henderson, a former officer (analyst) for the US Army, wrote the book *The Dark Visitor* and maintains the well-known Website of the same name, focusing on the activities of Chinese hackers.

194 Rich Barger, who is in charge of intelligence issues at Cyber Squared, served in the US Army (1st Information Operations Command). On the Cyber Squared Website, mention is made of the existence of many APT

among these commentators.[197] Because of the profile of a portion of its directors, we can also consider that the publications emanating from Mandiant also fit into this category. Indeed, before he set up the company in 2004, Kevin Mandia worked as part of the 7th Communications Group (Pentagon), as a Special Agent for AFOSI (U.S. Air Force Office of Special Investigations). Travis Reese and Dave Merkel, both members of the company's board of directors, are also former members of AFOSI. Richard Bejtlich, another member of Mandiant's board of directors, and founder of the Website Tao Security[198], was an intelligence officer in the U.S. Air Force CERT, as well as the Air Force Information Warfare Center (AFIWC) and the Air Intelligence Agency (AIA).

The publication of the report comes as the American authorities are engaged in a policy of toughening their positions in relation to cyberdefense: the announcement of the enhanced powers granted to Cyber Command[199], a

groups who are being analyzed by the company. [http://www.cybersquared.com/just-the-tip-of-the-iceberg/].

195 A member of Project 2049, and co-author of the report *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, M. A. Stokes served for 20 years in the US Air Force.

196 US Marine Lieutenant Colonel.

197 In China, the military is also the source of the majority of publications, which have profoundly marked western perceptions of China's ambitions and intentions over the course of the 2000s: the infamous Unrestricted Warfare preached by Colonels Liang Qiao and Wang Xiangsui. This publication has probably had more of an impact on western thinking than the equally important works relating to information warfare produced by other Chinese military figures (e.g. Wang Baocun, Dai Qingmin or Wang Pufeng) since the 1990s, but which have proved more confidential because of their more conceptual/theoretical nature and the language barrier. Liang Qiao, Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999, 228 pages, [http://www.cryptome.org/cuw.htm].

198 [http://taosecurity.blogspot.fr/].

199 Elisabeth Bumiller, *Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks*, The New York Times, 27 January 2013,

speech from the US Secretary of Defense about the need to protect the nation from cyber-attacks[200], President Obama's *Executive Order on Cybersecurity*[201], dialog at the highest level between the United States and China over the question of Cybersecurity[202], and toughening of the legal framework relating to cyber-warfare.[203]

Finally, the report has a place in an unusual economic context, which is extremely favorable for the Cybersecurity market (Mandiant's turnover for 2012, which is over 100 million USD, is up by 76% in comparison to the previous year).[204] The initiative does little to hide the commercial strategy of the enterprise: "Meet the Company That's Profiting from Chinese Hacking."[205] The conclusions advanced by the report therefore may not be as objective as may otherwise be thought, and may not reflect reality, but only one aspect of that reality, with the perspective having been chosen with commercial or political aims in mind.

[http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=0].

200 Leon A. Panetta, *Defending the Nation from Cyber-Attack*, Speech by the Secretary of Defense, New York, United States, 12 October 2012, [http://www.defense.gov/speeches/speech.aspx?speechid=1728].

201 White House, *Executive order on cybersecurity*, United States, 12 February 2013, [http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity].

202 Steve Holland, *Obama, China's Xi discuss cybersecurity dispute in phone call*, 14 March 2013, Reuters, [http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314].

203 Michael N. Schmitt (US Naval War College), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, April 2013, 300 pages.

204 Brad Stone, Michael Riley, *Mandiant, the Go-To Security Firm for Cyber-Espionage Attac*k, Bloomberg Business Week, 7 February 2013, [http://www.businessweek.com/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks#p2].

205 Matthew Yglesias, Meet the Company That's Profiting From Chinese Hacking, 19 February 2013, Slate.com, [http://www.slate.com/blogs/moneybox/2013/02/19/mandiant_is_the_big_winner_from_increased_anxiety_about_chinese_hacking.html].

These remarks lead us to consider all of the criticisms which have been leveled at the report, and the lessons that can be drawn from those criticisms.

The criticisms have come from China, based on clearly-defined arguments. The spokesman for the Foreign Ministry points the finger at the way in which the United States constantly levels accusations at China, saying that this type of approach is not helpful in solving the problem of cybercrime; that only international cooperation in the fight against cybercrime should be envisaged; that China too is one of the most prevalent victims of cyber-attacks; that the United States is the no. 1 source of those attacks, according to IP analysis; that China's legislation, which has been toughened in recent years, and Chinese policy, take a dim view of such practices; that on the international scene, China, along with Russia and a few other countries, has proposed a code of good conduct which has thus far been snubbed by the United States; and finally, the spokesman expresses surprise that it is technically possible to so precisely locate and attribute blame to the aggressors, as it is well known that they tend to carefully anonymize their operations.[206]

Other criticisms, however, have come from the United States[207] – particularly from the expert, Jeffrey Carr, first picking up on the numerous errors with which the dossier is fraught, and then the unsatisfactory methodology used. Thus, he points out:

---

206 *China opposes hacking allegations: FM spokesman*, XinhuaNet, 19 February 2013, [http://news.xinhuanet.com/english/china/2013-02/19/c_132178666.htm].

207 – Jeffrey Carr, *Mandiant APT1 Report Has Critical Analytic Flaws*, 19 February 2013, [http://jeffreycarr.blogspot.fr/2013/02/mandiant-apt1-report-has-critical.html#!/2013/02/mandiant-apt1-report-has-critical.html]. – Jeffrey Carr, *More on Mandiant's APT1 Report: Guilt by Proximity and Wright Patterson AFB*,http://jeffreycarr.blogspot.fr/2013/02/mandiant-apt1-report-has-critical.html#!/2013/02/more-on-mandiants-apt1-report-guilt-by.html].

– the mistakes made in terms of place names, in the localizing of the actors identified, with the main mistake being the statement that the district of Hebei is in Shanghai;

– the apparent bias of the authors. It seems that they refuse to acknowledge the possibility of the perpetrators of the attacks being anything other than Chinese, and even more specifically, the spies in Unit 61398. In this regard, Jeffrey Carr criticizes the company for not having validated its hypothesis (the Chinese origin of the attacks; the military identity of the attackers; the involvement of Unit 61398) by envisaging enough alternative scenarios. To do so, they need only have applied the methods used by the US intelligence agencies – for instance the tool known as ACH: Analysis of Competing Hypotheses. The fact of not having done so weakens the conclusions drawn in the report, leaving them open to criticism. The company is accused of having taken the easy way out, seeking to validate its own convictions and instincts, but at the cost of a lack of objectivity;

– the lack of precise definitions (what is an APT as spoken of by the report: is it a process, or the identity of the attackers)?

These criticisms cast doubt on the very quality of the document itself, the validity of its conclusions, and the impartiality of its authors.

Another criticism relates to the taking of undue risks. Revealing information about the investigative capacities used in the gathering of the data will inevitably lead the aggressors to alter their behavior, thereby (temporarily, at least) weakening the united states' security.[208] However, the company gives a certain amount of self-criticism in this

208 Ellyne Phneah, Embarassing China with reports won't aid security, ZDnet, 27 February 2013, [http://www.zdnet.com/cn/embarrassing-china-with-reports-wont-aid-security-7000011886/?s_cid=e305].

regard, explaining the choice within the report itself: it was felt that the publication of the truth merited this risk.

Whilst it does not truly provide any new information[209], and fails to prove the identity of the aggressors, the report does, in its own way, contribute to the alarmist discourse, conforms to the train of thought developed over more than 15 years: it stresses how dangerous the operations carried out by the Chinese intelligence unit are, confirms the existence of units of techno-warriors (high-tech spies much like those employed by America), and emphasizes the vulnerability of the American actors (by highlighting the number of recorded incidents and the relative ease with which the aggressors carry out their espionage operations). The "experts" belonging to the company channel the same fear mongering discourse, backed up by evidence. Of course (as is their trade), they propose solutions to defend against these threats.

The process of securitization[210] involves first identifying the threat (China, and its actions in cyberspace); naming the referential objects (critical infrastructures, companies, stability of the nation-State, western civilization, democracy, liberalism, cyberspace); next comes securitization proper,

209 The existence of Unit 61398 is not revealed by the Mandiant report. An article in the Chinese press (China Digital Times) made open reference to its existence in May 2004. The China Digital Times on 13 May 2004 stated that Unit 31398 of the Chinese army, located in the Pudong District in Shanghai, was recruiting computer specialists, and offering university study grants. Laura Saporito and James A. Lewis, *Cyber Incidents attributed to China*, CSIS, Washington, United States, 14 pages, 5 March 2013, [http://csis.org/files/publication/130311_Chinese_hacking.pdf]. The Project2049 Institute also published specific information about that unit in its November 2011 report. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao*, The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,* 11 November 2011, 32 pages, [http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf].

210 Theories of the Copenhagen School, security studies.

which entails the finding of solutions (cyberdefense policies, increasing of defensive and offensive resources, tightening of surveillance and control regulations, and commercial solutions).

In this process, the Cybersecurity firm is one of the key actors, on the side of the State, capable not only of offering solutions to the problems identified (protecting against the threat) but also of identifying and describing the threat. Thus, it has a significant degree of responsibility in the process of threat definition. The report and the criticisms of it demonstrate, once again, that, in spite of the effects of declarations, it is always possible to call the results into question, and put forward other, equally-credible hypotheses. The problem of attribution remains to be solved. However, though it may use uncertain results and debatable conclusions as a starting point, the technique still has an important part to play in the definition of a threat and (re)construction of a reality, which may have an impact not only from a commercial point of view (opening up new markets for (in)security) but also from a political standpoint (influencing the world view of the political decision-makers).

In the United States, a few rare critical voices are beginning to be heard – some of them calling for greater objectivity and discernment in the analysis of the threats (J. Carr and the various commentators on his blog about the Mandiant report; Eric C. Anderson in his Sino phobic discourse analysis[211]); others for greater restraint in the expression of the stakes in Cybersecurity policies (Martin Libicki, decrying America's warlike rhetoric, which runs the risk of triggering an uncontrollable escalation in international violence[212]). Yet we may also ask about how

211 Eric C. Anderson, *Sino phobia: the Huawei Story*, January 2013, Create Space Independent Publishing Platform, 400 pages, January 2013.
212 Kim Zetter, *Tone Down the Cyberwarfare Rhetoric, Expert Urges Congress,* Wired, 20 March 2013,

much counterweight can actually be carried by critical views and calls for caution, in the face of an alarmist discourse which is anchored in nearly two decades of propaganda painting the image of a major adversary.

8.1.6. *China, cyberspace and international relations*

China's might and its management of cyberspace are invariably of great importance in its international relations.[213] The emphasis in debates and analyses is placed on a few central topics.

China's use of cyberspace as a tool of power (John Oakley, 2011[214]; Sérgio Tenreiro de Magalhães, 2009[215]):

– the weight carried by China and its management of cyberspace in the national policies of security and defense (Ronald Deibert, 2010[216]; Jayson M. Spade, 2012[217]);

[http://www.wired.com/threatlevel/2013/03/tone-down-cyberwar-rhetoric/?utm_source=dlvr.it&utm_medium=twitter].

213 – Michael D. Swaine, *Chinese Views on Cybersecurity in Foreign Relations*, China Leadership Monitor, no. 42, 27 pages, June 23 2013, [http://media.hoover.org/sites/default/files/documents/CLM42MS.pdf].

– David Hanel, Chinese *Cybercrime – A Threat to the Occident? The Impact of Chinese Cybercrime on EU-China Relations*, University of Twente, 23th June 2013, 45 pages, [http://essay.utwente.nl/63300/1/Bachelor_Paper_Final_Version_d.hanel_s1062336.pdf].

214 John Oakley, *Cyber Warfare: China's strategy to dominate in cyber space*, University of Minnesota, 2011, 99 pages, [http://www.dtic.mil/dtic/tr/fulltext/u2/a547718.pdf].

215 Sérgio Tenreiro de Magalhães, Maria J. Rios,Leonel Santos, Hamid Jahankhani, *The People's Republic of China – The Emerging Cyberpower*, Communications in Computer and Information Science,Volume 45, 2009, ppp. 138–144.

216 Ronald Deibert, *China's Cyberspace Control Strategy: an overview and consideration of issues for Canadian policy*, Canadian International Council, February 2010, 18 pages, [http://cic.verto.ca/wp-content/uploads/2011/05/Chinas-Cyberspace-Control-Strategy-Ronald-Deibert.pdf].

– the relations, some of them hostile, between China and other nations; the impact of China's development of cyberwarfare capabilities (Yao-chung Chang, 2011[218]; Deepak Sharma, 2011[219]);

– the differing views between China and the Western countries, in terms of control of the Internet (Randolph Kluver 2005[220]; Ronald Deibert, 2010[221]; Milton L. Mueller, 2011[222]);

– the differences between China and the United States regarding Cybersecurity policies (Jayson M. Spade, 2011[223];

217 Jayson M. Spade, *China's cyber power and America's National Security*, US Army War College, 81 pages, 2012, [http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf].

218 Yao-chung Chang, *Cyber Conflict Between Taiwan and China*, Strategic Insights, Spring 2011, pp. 26–35, [http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI-v10-I1_Chang.pdf].

219 Deepak Sharma, *China's Cyber Warfare Capability and India's Concerns,* Journal of Defence Studies, Vol. 5, No 2. April 2011, pp. 62–76, [http://www.idsa.in/system/files/jds_5_2_dsharma.pdf].

220 Randolph Kluver, *US and Chinese expectations of the Internet*, China Information, XIX; 2, pp. 299-324, 2005, [http://www.asc.upenn.edu/usr/ogandy/c734%20resources/kluver-uschinapolicyexpectationsinternet.pdf].

221 Ronald Deibert, *China's Cyberspace control strategy: an overview and consideration of issues for Canadian policy*, Canadian International Council, China Papers n°7, 18 pages, February 2010, [http://cic.verto.ca/wp-content/uploads/2011/05/Chinas-Cyberspace-Control-Strategy-Ronald-Deibert.pdf].

222 Milton L. Mueller, *China and Global Internet Governance, A Tiger by the Tail*, Chapter 9, pp. 177–194, in R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (eds.) *Access Contested: Security, Identity and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press, 2011, [http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-09.pdf].

223 Jayson M. Spade, *China's cyber power and America's national security*, US Army War College, 2011, 81 pages, [http://www.carlisle.army.mil/dime/documents/China's%20Cyber%20Power%20and%20America's%20National%20Security%20Web%20Version.pdf].

Viktor Nagy, 2012[224]; Alistair D. B. Cook, 2013[225], etc.). The approach is generally to describe Sino-American relations as difficult, problematic, with the potential to cause crises or conflicts (Wilson Vorn Dick, 2013[226]; etc.), although a few speeches, articles and studies point out that the dialog about cyberspace is in the process of being established[227] between the two powers, particularly by way of bilateral military initiatives. Thus, according to Wilson Vorn Dick, this "problem" has a number of facets:

– first and foremost, it is rooted in China's practices (cyber-attacks) and in the stance of the authorities in Beijing, who consistently deny the facts,

– China's lack of experience in the practice of laws of armed conflict: "*One crucial point lost amid the backdrop of the new digitized battlefield is the lack of Chinese leadership experience both military and political in utilizing key principles of the laws of armed conflict (LOAC)*". On the legal level, there is a significant imbalance. The United States has experience of the law, of its application, and (according to the author), of respecting *Jus in Bello*. However, an

224 Viktor Nagy, *The geostrategic struggle in cyberspace between the United States, China, and Russia*, AARMS, Vol. 11, No. 1 (2012) 13–26, [http://www.konyvtar.zmne.hu/docs/Volume11/Issue1/pdf/02.pdf].

225 Alistair D. B. Cook, *The cybersecurity challenge and China-US relations*, EAI Background Brief, No. 828, 20 June 2013, 3 pages, [http://www.eai.nus.edu.sg/BB828.pdf].

226 Wilson Vorn Dick, *The Real U.S.-Chinese Cyber Problem,* The National Interest, July 30, 2013, [http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796].

227 – *Bilateral Discussions on Cooperation in Cybersecurity China*, Institute of Contemporary International Relations (CICIR) – Center for Strategic and International Studies (CSIS), June 2012, 4 pages, [http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf].

– C. Raja Mohan, *US-China Cyber Talks: Internet Security in the Global Economy*, RSIS, Singapore, RSIS Commentaries, n°046/2013, 18 March 2013, 2 pages, [http://www.rsis.edu.sg/publications/Perspective/RSIS0462013.pdf].

interpretation error, an improperly-controlled action with unforeseen consequences, could put the spark to the powder keg. The risk is of the escalation of force, and of violence.[228]

These debates focusing on cyber-issues fit in with the broader question of the conditions of the ratio of strength between the two powers (David C. Gompert, 2011[229]), of which cyber is, ultimately, only one aspect, but one which causes numerous genuine tensions between the two states. Besides, adding cyberwarfare to the list of points of discord between China and the United States is, undoubtedly, not the best way to achieve better *entente* between the two states.[230]

In this context, it is rare to hear voices which attempt to relativize the significance of this specific threat: "*Despite the PLA's interest in and preparations for cyber operations, and the importance of networks to military operations, open source evidence does not justify the conclusion that the PRC is a threat per se. Much of what has been classified as a cyber-attack is not hostile at all and is actually clandestine spying and a form of intelligence gathering inside computer networks. Hackers, China's internal security threat, are likely their first and foremost priority.*"[231]

228 The author refers to the American official document: Army's *Escalation of Force Handbook.*

229 David C. Gompert, Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability*, Center for Study of Chinese Military Affairs, and National Defense University Press; Washington, 2011, 236 pages, [http://ndupress.ndu.edu/Portals/68/Documents/Books/paradox-of-power.pdf].

230 Ting Xu, China and the United States: hacking away at cyber warfare, East-West Center, Asia Pacific Bulletin, n°135, November 1, 2011, 2 pages,
[https://www.eastwestcenter.org/sites/default/files/private/apb135_1.pdf].

231 Ammilee A. Oliva, *China: Paper Tiger in Cyberspace*, 17 May 2012, 46 pages, [http://www.stormingmedia.us/54/5456/A545665.html].

8.1.7. *Particular points from the Western perspective*

Westerners are not capable of understanding Chinese society.[232] This idea is formulated not by the Chinese, but by Westerners themselves.

Westerners have difficulty in comprehending the complex nature of modern China, because it does not fit into any of the typical categories. Tzvetan Todorov[233] summarizes this complexity in the following terms: "*China no longer corresponds to the "ideal model" of a totalitarian regime. Rather, to outside observers, China appears to be a baroque hybrid of communist rhetoric, represessive centralized administration and a market economy which allows, or even favors (something which would have been inconceivable in the time of Soviet and Maoist communism) openness to the outside world and enrichment of individuals.*" The published analyses often dwell on the differences.[234]

Without appropriate referential frameworks to aid comprehension, for example, Westerners cannot understand why a society which frequently rises up against injustices does not rise up against the governing regime at the same time; why that society speaks out against corruption and embezzlement, but continues to have faith in its leaders.

Indeed, if we Westerners do not understand, affirms Jean-Louis Rocca, it is because our analytical filter yields nothing but contradictions. We would first be convinced that a

232 Jean-Louis Rocca, *Pourquoi nous ne comprenons pas la société chinoise*, p. 5, in Emilie Frenkiel, Jean-Louis Rocca (*eds.*), *La Chine en mouvements*, Presses Universitaires de France, 2013, 100 pages.
233 Tzvetan Todorov, *Les ennemis intimes de la démocratie*, Le Livre de Poche, Robert Laffont, Paris, 2012, 284 pages.
234 "Russia and China have different conceptual models for cyber agreements". Christopher Ford, *The Trouble with Cyber Arms Control*, Hudson Institute, September 2011, [http://www.hudson.org/files/publications/20110301_TNA29Ford.pdf].

democratic market is the only envisage able prospect; yet the culturalist paradigm speaks of the existence of a "Chinese model", a specific approach, a particular channel, which is entirely defined. From this point of view, there would only seem to be solutions "*à la chinoise*", different from our own. Interpretations of China thus hesitate between these two paradigms: thus, in order to discuss China's political evolution, we say that it does not conform to the single model which is becoming widely adopted on the international scene (democracy), but we also accept that the switch to democracy in China may first require a political modernity "*à la chinoise*", a transition to democracy or another form of democracy.[235] Hence, analyses of China are constrained by the two paradigms (conformity to the Western democratic model; and the culturalist model).

These two paradigms are also found in the discourse produced about Chinese cyber strategy:

– China is far removed from the democratic model (there is control and censorship of the Internet in China), but also more generally from usages in accordance with the rules set by the international community. By placing emphasis on the lack of respect for these international rules with regard to espionage, the United States paint a picture of China which is outside of the "norms" which are becoming those of the modern international scene. The Chinese themselves appear to place themselves outside of this system, beyond the governance of these rules: after all, they published "Unrestricted Warfare", meaning the usage of all kinds of technological tools in all directions, in contravention of the norms of international deontological laws or rules? By the principle of this contrast between an innocent (Western)

235 Jean-Louis Rocca, *Pourquoi nous ne comprenons pas la société chinoise*, p. 5, in Emilie Frenkiel, Jean-Louis Rocca (eds.), *La Chine en mouvements*, Presses Universitaires de France, 2013, pp. 5–6.

democracy and authoritarianism[236], measures taken by China would be condemnable (censorship, cyber surveillance), whereas those taken by democracies would be legitimate (cyber surveillance is a necessity for the maintaining of peace in a democracy). Could it be that the arguments are exaggerated when it comes to China? Do we lose some of the necessary objectivity? If this is so, however, is the problem limited to discourse about China or is it more general in discourse about Cybersecurity? Does the discourse about the cyber threat represented by the Chinese hacker accurately reflect the reality, or is it exaggerated?

– in addition, analysts also emphasize the development of a specifically Chinese channel, and have no hesitation in drawing the connection between ancient Chinese philosophy and modern thought (e.g. viewing China's cyberdefense strategies and doctrines as deriving directly from Sun Tzu's strategy). Western authors even affirm that China, because of its culture, its way of thinking, its philosophy, and its tradition, might be better prepared for cyberconflict than other nations in the world. Culturalism appears to be a practical way of explaining the Chinese exceptionality, as that country's culture has always been deemed different, "separate".[237] Yet that uniqueness is not only to be understood in a negative light. We can hold up the difference as a model from which it would be wise to draw inspiration (e.g. by first understanding and then transposing the seminal principles laid down by Sun Tzu to our own culture, our own strategy).

236 Jean-Louis Rocca, *Pourquoi nous ne comprenons pas la société chinoise*, p. 5, in Emilie Frenkiel, Jean-Louis Rocca (eds.), *La Chine en mouvements*, Presses Universitaires de France, 2013, 100 pages.
237 Jean-Louis Rocca, *Pourquoi nous ne comprenons pas la société chinoise*, p. 5, in Emilie Frenkiel, Jean-Louis Rocca (eds.), *La Chine en mouvements*, Presses Universitaires de France, 2013, pp. 14–15.

Thus, our referential framework oscillates between two limits whereby China is an outsider, a "different" actor. This fundamental postulate greatly constrains any analysis, and is visible in the discourse published about China; "cyber" issues, security and defense are no exception to this phenomenon.

8.2. The evolution of American discourse about China, Cybersecurity and cyberdefense

We can gain an insight into American discourse and its evolution by analyzing three corpora: the Defense Department's annual reports, relating to the evolution of China's defense; the speeches given by the US Secretaries of Defense; and the prospective exercises carried out by the National Intelligence Council and published every four years. This corpus is not a reflection of the whole of American thinking, which would of course also be reflected through other political discourse (White House communiqués, Congress, GAO reports, etc.), the media, research publications, or websites, blogs, social media in the broadest sense. However, we have chosen to limit our corpus to these three sources, because we believe they give a fairly accurate illustration of the discourse of the dominant actors, which are capable of influencing political decision-making. Finally, these corpora have been chosen because they are easy to access (available on the Internet in their entirety), and for the period which they cover (the past two decades), which serve our objective here, i.e. to demonstrate the main arguments in the discourse and the evolution of those arguments over time.

8.2.1. *The annual reports of the US Defense Department*

As stipulated by the National Defense Authorization Act for Fiscal Year 2000, Section 1202, Public Law 106-65, amended by Section 1246, "Annual Report on Military and Security Developments Involving the People's Republic of China", of the National Defense Authorization Act for Fiscal Year 2010, Public Law 111-84, the Defense Department annually delivers a report to Congress on the progression of Chinese military power. Two versions of this annual report are produced: one which is not classified, which is available online on the Defense Department's Website; the other which is classified. The report must focus on four aspects of the development of Chinese defense: its technological, strategic, organizational and conceptual dimensions. Finally, the report must not merely give overviews and observations, but rather must convey a prospective vision, all from the viewpoint of US/China relations, and of cooperation on issues of security.

The first report published in 2002[238] spoke of information operations and information warfare, and highlighted the strategic nature of those two concepts in Chinese defense policy: "*China views information operations/information warfare (IO/IW) as a strategic weapon foruse outside of traditional operational boundaries*". Information space, which would later be called "cyberspace", had a leveling effect: "*China is particularly sensitive to the potential asymmetric applications IO/IW can have in any future conflict with a technologically superior adversary*". China was paying particular attention to IO and IW: "*Both the Academy of Military Science and the National Defense University have published several books devoted, in part or*

238 Department of Defense, *Annual Report on the Military Power of the People's Republic of China,* Washington, 56 pages, 2002, [http://www.defense.gov/news/jul2002/d20020712china.pdf].

completely, to this subject. These writings indicate a growing sophistication in the PLA's understanding of all aspects of IO". It was evident even at that point that China, like the United States, was integrating the use of ICT into military affairs: "*China is pursuing IO/IW development as part of its overall military modernization. Combining information warfare--such as computer hacking--with irregular special and guerilla operations, would allow China to mount destructive attacks within the enemy's own operations systems, while avoiding a major head-on confrontation*", with both an offensive and defensive objective: "*Efforts have focused on increasing the PLA's proficiency in defensive measures, most notably against the threat of computer viruses […] Increases in network defense likely will enhance China's understanding of virus propagation and behavior, creating a solid knowledge base not only for computer network defense (CND), but potentially also for computer network attack(CNA) through malicious software development*".

The report also highlighted China's initiatives in terms of R&D in the domain, and the method of taskforce construction (in terms of human resources), based on using reserves of specialists – a method which would later be used by other countries: "*In an effort to improve its skill base in the IT field, the PLA has been recruiting specialists via its reserve officer selection program*".

In spite of these efforts, the US felt that China did not yet have the means to penetrate the most heavily protected networks: "*China has the capability to penetrate poorly protected U.S. computer systems*", but that did not take away from the potential danger it posed: China "*potentially could use CNA to attack specific US civilian and military infrastructures*".

The development of nationalistic hacking added to the concerns created by the rise in power of China's military capabilities, especially as the government could be

supporting this kind of action: "*In the near term, nationalistic hacking is likely to occur during periods of tension or crises. Chinese hacking activities likely would involve extensive web page defacements with themes sympathetic to China. Although the extent of Chinese government involvement would be difficult to ascertain, official statements concerning the leveraging of China's growing presence on the Internet, and the application of the principles of "People's War" in "net warfare", suggest the government will have a stronger role in future nationalistic hacking*".

The 2003 report[239] again deals with the same topics, but goes into greater depth. It again mentions the role of IO and IW in Chinese strategy, with these concepts notably encompassing "*computer warfare, network warfare, temporal-spatial analysis, knowledge warfare, information protection, and electronic security*". The concept of IO is therefore a complex construct: it includes "*elements such as combat secrecy, military deception, psychological warfare, electronic warfare, physical destruction of C2 infrastructure, and computer network warfare*". Above all, though, according to the United States, these IOs are, for China, a pre-emptive weapon, a non-conventional weapon, for asymmetrical conflicts.

The 2003 report also reiterates the importance of reserve units in the organization of IOs and IW, and states that China is setting up specialized units, in various cities throughout the country, thus forming a corps of cyber-warriors: "*Specialized IO/IW reserve units are active in several cities developing "pockets of excellence" that could gradually develop the expertise and expand to form a corps of "network warriors" able to defend China's*

239 Department of Defense, *Annual Report on the Military Power of the People's Republic of China,* Washington, 28 July 2003, 52 pages, [http://www.defense.gov/pubs/2003chinaex.pdf].

telecommunications, command, and information networks, while uncovering vulnerabilities in foreign networks".

According to the same report, the Chinese army possessed the means to carry out attacks on networks in armed conflicts: "*Special information warfare units could attack and disrupt enemy C4I, while vigorously defending PRC systems*".

The 2004 report[240] estimates that China's IO capabilities are expanding and improving, although its "*equipment is dated and does not appear to be readily available to most units*". However, the report predicts that: "*domestic production, along with foreign technology transfers, probably will give the PLA access to a wider range of modern equipment in the future*". It also states that: "*China is experiencing a rapid buildup of its information technology capabilities*". The rapidity of Chinese technological progress is founded largely on the acquisition of foreign technologies, technology transfers, knowledge-sharing, the installation in China of R&D centers for foreign companies, and the creation of joint ventures. Economic, industrial and research partnerships are thus helping speed up the process of modernization of the Chinese army.

One of the central subjects around which the American analysis pivots is the relationship between China and Taiwan, and the potential for that situation to evolve into an armed conflict. The scenario of this conflict thus serves as the background for the argument about Chinese development of IW capabilities, and is used to demonstrate the pertinence of the concerns formulated by the American observers: "*During a cross-Strait conflict, China most likely would initiate an intensive perception management*

240 Department of Defense, *Annual Report on the Military Power of the People's Republic of China,* Washington, 2004, 54 pages, [http://www.defense.gov/pubs/d20040528prc.pdf].

campaign, with both global and regional audiences, to reduce the desire of Taiwan to resist, justify China's military campaign, and deter U.S. intervention". Indeed, by controlling that information space, China would have the possibility to act quickly, to win a victory by playing with public perceptions (which are gold dust in psychological operations), and attacking the critical infrastructures and command systems of the enemy country. China could use information space to its advantage at every stage of the offensive operation: "*China anticipates that this strategy will succeed because of the fragility of the Taiwan population's psychology. The Chinese perception management campaign most likely would use Chinese, Hong Kong, Taiwan, and other regional media to deliver messages to the Taiwan people and leaders. Unclassified Chinese writings reveal that attacking C4I systems, civilian information technology, and communication infrastructure are critical for gaining information superiority. Prior to an attack, Chinese information operations personnel and special forces or espionage agents most likely would gain and maintain access to such communication nodes for intelligence exploitation and disrupt critical infrastructure, such as the power grid and vulnerable collocated military and civilian telecommunications. Exploiting other portions of the information operations spectrum (through electronic warfare and denial and deception) also could disrupt Taiwan's defenses, and attacks against unclassified DoD computer networks related to logistics could delay U.S. efforts to intervene*".

China's capabilities are deemed entirely sufficient to be able to carry out operations against Taiwan. The report notes that Taiwanese experts have suggested their armed forces begin to prepare for this new kind of attack. Taiwan has high-level technologies and high-level engineers at its disposal, and can use them for its cyberdefense.

The 2005 report[241] speaks not of "cyber", but rather of "information technologies" and "Computer network operations". The report highlights the emergence of a new expression in China's vocabulary surrounding defense: "*China's latest Defense White Paper deployed authoritatively a new doctrinal term to describe future wars the PLA must be prepared to fight: "local wars under conditions of informationalization". This term acknowledges the PLA's emphasis on information technology as a force multiplier and reflects the PLA's understanding of the implications of the revolution in military affairs on the modern battlefield"*. This formulation defines the extent of the Chinese use of IW capabilities, whose development is continuing apace: "*The PLA continues to improve its potential for joint operations by developing a modern, integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) network and institutional changes*".

The report describes the components of information operations using a referential framework which is very similar to that employed by the US Department of Defense, notably distinguishing between CNO[242], CNA[243], CNE[244] and CND[245]: "*China's computer network operations (CNO) include computer network attack, computer network defense, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and "electromagnetic dominance" early in a conflict, and as a force multiplier*".

Specialists in Chinese affairs speak of the Chinese technique of *Integrated Network Electronic Warfare*. The report also stresses the lack of a formal Chinese doctrine

241 Department of Defense, *The Military Power of the People's Republic of China 2005*, Washington, 2005, 52 pages, [http://www.defense.gov/news/jul2005/d20050719china.pdf].
242 Computer network operations.
243 Computer network attacks.
244 Computer network exploitation.
245 Computer network defense.

concerning operations in cyberspace. This lack of official references, of a publically-available doctrine, destabilizes the United States, who must continue to pressure China to communicate about its projects, developments, capabilities, doctrines, etc., as the US does.

The 2006[246], 2007[247], 2008[248], 2009[249] and 2010 reports[250] reiterate the observations on the same points:

– China is continuing its development of military capabilities:

- "*China is likely to continue making large investments in high-end, asymmetric military capabilities, emphasizing electronic and cyber-warfare*",[251]

- this development project includes the expansion of the available human resources and the organization of armed forces: "*The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to*

246 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2006*, Washington, 58 pages, [http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf].
247 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2007*, Washington, 50 pages, [http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf]
248 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2008*, Washington, 66 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].
249 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2009*, Washington, 78 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf]
250 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2010*, Washington, 83 pages, [http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf].
251 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2006*, Washington, 58 pages, [http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf].

incorporate offensive CNO into its exercises, primarily in first strikes against enemy networks";[252]

– the reserves and militias are playing an essential role in the constitution of IW forces:

- "*Formation of Information Warfare Reserve and Militia Units. The Chinese press has discussed the formation of information warfare units in the militia and reserve since at least the year 2000. Personnel for such units would have expertise in computer technology and would be drawn from academies, institutes, and information technology industries […] Militia / reserve personnel would make civilian computer expertise and equipment available to support PLA military training and operations, including "sea crossing," or amphibious assault operations. During a military contingency, information warfare units could support active PLA forces by conducting "hacker attacks" and network intrusions, or other forms of "cyber" warfare, on an adversary's military and commercial computer systems, while helping to defend Chinese networks*";[253]

– the reports give observations about the Chinese IW strategy, and the definition of IW, stressing its offensive, preemptive, and anti-access function:

- "*The PLA considers active offense to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the*

252 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2007*, Washington, 50 pages, [http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf]
253 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2006*, Washington, 58 pages, [http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf].

PLA could employ information warfare preemptively to gain the initiative in a crisis",[254]

- "*The PLA is also building capabilities for information warfare, computer network operations, and electronic warfare, all of which could be used in preemptive attacks*"[255]. *This strategy entails taking the initiative by going on the offensive. "PLA authors describe preemption as necessary and logical when confronting a more powerful enemy […] An effective defense includes destroying enemy capabilities on enemy territory before they can be employed […] China is pursuing this ability by improving information and operational security, developing electronic warfare and information warfare capabilities, and denial and deception*",[256]

- the analysis again uses the Americans' referential framework to define the concept of "Computer Network Operations" (comprising CNE, CAN and CND), and the expression "Integrated Network Electronic Warfare" (2006, 2007 and 2008 reports)is used to denote the integration of electronic warfare, CNO and kinetic strikes against C4 centers. According to the 2008 report, the integration of CNO into military maneuvers began in 2005,

- "*China's continued pursuit of area denial and anti-access strategies is expanding from the traditional land, air,*

254 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2006*, Washington, 58 pages, [http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf].
255 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2007*, Washington, 50 pages, [http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf].
256 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2007*, Washington, 50 pages, [http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf].

and sea dimensions of the modern battlefield to include space and cyber-space".[257]

In 2008[258], the report alludes to the cyber-attacks originating in China, affecting networks all over the world:

– "*In the past year, numerous computer networks around the world, including those owned by the U.S. Government, were subject to intrusions that appear to have originated within the PRC*."[259] Although the attacks require particular capabilities and skills, there is, as yet, nothing to unequivocally indicate that they were the work of the Chinese army. Yet the very mention of the possibility of the Chinese army's involvement is, in itself, a thinly-veiled accusation: "*Although it is unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC government, developing capabilities for cyberwarfare is consistent with authoritative PLA writings on this subject*".[260] The report also mentions other actors on the international scene who have openly laid blame at China's door: "Hans Elmar Remberg, Vice President of the German Office for the Protection of the Constitution (Germany's

257 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2007*, Washington, 50 pages, [http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf].
258 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2008*, Washington, 66 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].
259 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2008*, Washington, 66 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].
260 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2008*, Washington, 66 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].

domestic intelligence agency), publicly accused China of sponsoring computer network intrusions "*almost daily*"[261].

The 2009 report[262] introduces the notion of cyber-warfare. The chapter entitled "Cyber-warfare" discusses the cyber-attacks suffered by the US government, which are suspected (though cannot be proven) to have been carried out by the Chinese authorities. The report cites a number of cases of cyber-attacks recorded the world over (India, Belgium, the US), indicating the extent of the phenomenon: this is not merely a question of conflict between China and the United States.

The 2010[263] and 2011[264] reports take the same approach, citing a number of cyber-attacks recorded all over the world. These operations are classified as espionage activities, because the factor they have in common is the exfiltration of (often sensitive) data – e.g. strategic or military data. Although the 2010 report speaks of "cyber-warfare", it often comes back to the notion of "IW", and its psychological dimension, encompassed within the concept of the "Three Warfares" – a concept developed specifically by the Chinese army: "*In 2003, the CCP Central Committee and the CMC approved the concept of "Three Warfares" (san zhong zhanfa), a PLA information warfare concept aimed at influencing the psychological dimensions of military activity*". These "three

261 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2008*, Washington, 66 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf].
262 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2009*, Washington, 78 pages, [http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf].
263 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2010*, Washington, 83 pages, [http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf].
264 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2011*, Washington, 94 pages, [http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf].

warfares" include Psychological Warfare, Media Warfare, and Legal Warfare. "*The concept of the "Three Warfares" is being developed for use in conjunction with other military and non-military operations.*"

The 2011 report[265] defines what the United States views are the potential uses of the Chinese cyber capabilities: "*Cyberwarfare capabilities could serve PRC military operations in three key areas. First and foremost, they allow data collection through exfiltration. Second, they can be employed to constrain an adversary's actions employed to constrain an adversary's actions based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict*". It also identifies sources of the Chinese doctrine – specifically two publications which have caught the attention of the American analysts: Science of Strategy and Science of Campaigns.

The question of cyberdefense cannot be reduced to the development of cyber capabilities and computer network operations. China is making an effort in the area of diplomacy by participating in multilateral and international fora, where it is often aligned with Russia – particularly in terms of promoting a vision of Internet governance. The United States is unhappy that China has not yet come around to its (the US) point of view, and accepted the application of international humanitarian law and the laws of war in cyberspace. Although it deals with cyber capabilities, the 2011 report preserves the notion of "IW", highlighting the continuity of the Chinese policy of developing its capabilities in this domain for more than 10 years previously: "*China is pursuing a variety of air, sea, undersea, space, counter space, information warfare systems,*

265 Department of Defense, *Military and Security Developments Involving the People's Republic of China 2011*, Washington, 94 pages, [http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf].

and operational concepts to achieve this capability, moving toward an array of overlapping, multilayered offensive capabilities extending from China's coast into the western Pacific. [...] China is improving information and operational security to protect its own information structures, and is also developing electronic and information warfare capabilities, including denial and deception, to defeat those of its adversaries". Later on in the same chapter, we find the same elements which have consistently been appearing since 2002, i.e., those relating to capability development, human resources, reservists, and strategic elements (CNO, CAN, CND and CNE).

In the 2012 report[266], the notions of Information Warfare and Information Operations are absent this time.

The emphasis is again placed on the development of China's capabilities: "*In addition to the direct-ascent anti-satellite weapon tested in 2007, these counter space capabilities also include jamming, laser, microwave, and cyber weapons*". At the heart of the concerns is the issue of cyber-espionage, in a section entitled "*Cyber-espionage and Cyberwarfare Capabilities*", which begins by recapping the cyber-attacks carried out in 2011, stressing the nature of the targets affected. Up until then, the government's and the army's systems had been targeted. The report eagerly points out that private businesses have now fallen prey to the same operations. These allusions are reminiscent of the accusations of economic espionage carried out by the Chinese army for the benefit of the nation's companies. These practices, which the US condemns, compound the differences of opinion regarding the means of governance of cyberspace. A section is given over to the economic espionage carried out

266 Department of Defense, *Annual Report to Congress. Military and Security Developments Involving the People's Republic of China 2012*, Washington, 52 pages, [http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf].

by China, recalling that, of course, at least a dozen different nations conduct similar operations against the United States. China, however, appears to be the most active and the most persistent offender: "*Chinese actors are the world's most active and persistent perpetrators of economic espionage*".

The 2013 report[267] touches on at least four aspects of cyberdefense: the developing Chinese power; the notions of pre-emptive weapons, informational superiority and asymmetry; economic cyber-espionage; and the code of conduct in the area of security.

China is firstly depicted as a power which has been in the process of development for over 10 years, but is now operational, according to the 2013 report: "*The PLA has made huge progress in developing information technology and realizing information integration in recent years.*"[268] China is investing in the development of technological and cyber capabilities: "*Beijing is investing in military programs and weapons designed to improve extended-range power projection and operations in emerging domains such as cyber, space, and electronic warfare*."

The PLA's operations are considered as pre-emptive action weapons, with the aim of achieving informational superiority; this would enable China to combat superior adversaries (asymmetrical conflict, the equalizing nature of cyberspace). This informational superiority also contributes to its so-called Anti-Access/Area Denial (A2/AD) capabilities.

---

267 Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2013, Office of the Secretary of Defense, Washington, 92 pages, 2013, [http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf].

268 Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2013, Office of the Secretary of Defense, Washington, 92 pages, 2013, [http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf].

The report points out that in 2010, in *China's 2010 Defense White Paper,* the PCR itself expressed concern over the cyberwarfare programs run by foreign nations. Each party (the US, China and other nations) thus believes itself to be in the right in its cyberdefense projects and measures, because the strategy is shared by all the major actors on the international stage.

According to the US Department of Defense, the development of cyber capabilities for warfare is consistent with Chinese military doctrine. The report, once again, draws on two reference documents from the Chinese body of strategic literature: *Science of Strategy* and *Science of Campaigns*. These two texts refer to information warfare, rather than cyber-operation directly.

The finger is also pointed at China for its practices of economic cyber-espionage, aimed at obtaining advanced foreign technologies: "*Numerous computer networks, including those owned by the US government, were targeted for intrusion, some of which were attributable to the Chinese government and military*."[269] The accusation is direct: "*China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs."*

China, along with Russia, is also internationally promoting its proposed *Information Security Code of Conduct*, which is intended to affirm the principle of exercising of the right of sovereignty over content and information flow.

---

269 *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2013*, Office of the Secretary of Defense, Washington, 92 pages, 2013, [http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf].

All of this makes China a threat. Firstly, its technological capabilities in cyberspace (which give China the means to carry out offensive operations); and secondly the anti-access strategy is a threat to the freedom of projection of the American forces in the Pacific region. These observations have been being formulated since the beginning of the 2000s by the United States. China's practices (economic cyber-espionage) and its objectives (the Code of Conduct) are contrary not only to the United States' interests (of course), but also its values. There is a significant difference of opinion on these points.

8.2.2. *Speeches of the Secretaries of Defense*

China has essentially been part of the discourse of the US Secretaries of Defense from the start of the 2000s. Chronologically, this corresponds to the date of establishment of the annual reports on Chinese military development produced by the Department of Defense, in accordance with the *National Defense Authorization Act for Fiscal Year 2000*, Section 1202, Public Law 106-65.

Whilst, in general terms, the speeches of the successive Secretaries of Defense between 1995 and 2014 increasingly discuss the issue of "cyber", when we analyze the whole of the available corpus, we can see that China is not remotely associated with that issue until 2008, but that from that point on, the China issue becomes more apparent. Thus, between 2000 and 2007, the Chinese are mentioned essentially because of the concerns that they raise:

– because of the increasingly important role China is assuming on the international stage, and the uncertain prospects for its evolution: "*…I don't think it's written exactly how they're going to enter the world, goodness knows all the countries in the region and in the world are working to try to*

see that they enter the global community in a peaceful, rational way, without any grinding of gears";[270]

– there are many unknowns in the equation – particularly in relation to the true efforts made by China in terms of military development, and in relation to China's intentions (is this development of capability for peaceful or aggressive ends?): "*Among other things, the report concludes that China's defense expenditures are much higher than Chinese officials have published. It is estimated that China's is the third largest military budget in the world, and clearly the largest in Asia. China appears to be expanding its missile forces, allowing them to reach targets in many areas of the world, not just the Pacific region, while also expanding its missile capabilities within this region. China also is improving its ability to project power, and developing advanced systems of military technology. Since no nation threatens China, we must wonder: Why this growing investment? Why these continuing large and expanding arms purchases? Why these continuing robust deployments? Though China's economic growth has kept pace with its military spending, it is to be noted that a growth in political freedom has not yet followed suit. With a system that encouraged enterprise and free expression, China would appear more a welcome partner and provide even greater economic opportunities for the Chinese people*";[271]

– the nature of the diplomatic relations, when an incident occurs between the two countries: "*A few months ago, as we all know, an unarmed EP-3 reconnaissance aircraft flying in*

270 *AUSA Air, Space, and Missile Defense Symposium,* Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld, via video teleconference, Wednesday, December 10, 2003, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=595].

271 *International Institute for Strategic Studies*, Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld, Shangri-La Hotel, Singapore, Saturday, June 04, 2005, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=77].

the airspace over the China Sea was struck by a Chinese fighter and, of course, for a while we had 24 of our great personnel detained. Some ask why are we conducting surveillance against another nation? My answer to that is, "That's what we do." We are vigilant, we are watchful because we know that our interests and those of our allies in the region may be challenged and we must be ready";[272]

– generally speaking, the United States criticize the Chinese approach for its opacity, the lack of transparency regarding China's intentions and methods, and wonders about the effect such a stance might have on international relations: "*China has a strong economic growth rate today and an industrious workforce. But there are aspects of China's actions that can complicate their relationships with other nations. As we discussed last year, a lack of transparency with respect to their military investments understandably causes concerns for some of their neighbors*."[273]

Regardless of the concerns, and of the developments of capabilities, the Secretary of Defense points out that the Sino-American relation cannot be envisaged as a hostile one: "*I disagree with those who portray China as an inevitable strategic adversary of the United States*."[274]

---

272 *Testimony before the House Appropriations Committee: Fiscal Year 2002 Defense Budget Request,* As Delivered by Secretary of Defense Donald H. Rumsfeld, Chairman of the Joint Chiefs of Staff General Hugh Shelton, Rayburn House Office Building, Washington, DC, Monday, July 16, 2001, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=408].

273 *International Institute for Strategic Studies Conference*, As Delivered by Secretary of Defense Donald H. Rumsfeld, Shangri-La Hotel, Singapore, Saturday June 3 2006, Saturday June 03 2006, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=11].

274 Keio University, As Delivered by Secretary of Defense Robert M. Gates, Keio University, Tokyo, Japan, Friday, January 14, 2011, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1529].

Although this statement was made in 2011, from 2008 onwards the discourse has evolved. China has become a more openly apparent threat by virtue of the level of its defense capabilities: "*In the case of China, investments in cyber-and anti-satellite warfare, anti-air and anti-ship weaponry, submarines, and ballistic missiles could threaten America's primary means to project power and help allies in the Pacific: our bases, air and sea assets, and the networks that support them*."[275] Now, therefore, the question of Chinese cyberwarfare capabilities arises.

The remarks were repeated in very similar terms the following year: "*As we know, China is modernizing across the whole of its armed forces. The areas of greatest concern are Chinese investments and growing capabilities in cyber-and anti-satellite warfare, anti-air and anti-ship weaponry, submarines, and ballistic missiles*."[276] Rather than the capabilities for symmetrical conflict, cyberdefense contributes to the Chinese anti-access strategy, thus endangering America's abilities to project power and intervene in the Pacific region: "*In fact, when considering the military-modernization programs of countries like China, we should be concerned less with their potential ability to challenge the U.S. symmetrically – fighter to fighter or ship to ship – and more with their ability to disrupt our freedom of movement and narrow our strategic options. Their investments in cyber and anti-satellite warfare, anti-air and anti-ship weaponry, and ballistic missiles could threaten America's primary way to project power and help allies in the*

275 *National Defense University (Washington, D.C.),* As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Monday, September 29, 2008,
[http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1279].
276 *Submitted Statement on DoD Challenges to the Senate Armed Services Committee,*As Submitted by Secretary of Defense Robert M. Gates, Room SD-106, Dirksen Senate Office Building, Washington, D.C., Tuesday, January 27, 2009, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1337].

Pacific – in particular our forward air bases and carrier strike groups. This would degrade the effectiveness of short-range fighters and put more of a premium on being able to strike from over the horizon – whatever form that capability might take."[277]

This concern did not disappear, because in 2011 the Secretary of Defense put forward the same arguments: "*As I alluded to earlier, advances by the Chinese military in cyber and anti-satellite warfare pose a potential challenge to the ability of our forces to operate and communicate in this part of the Pacific. Cyber-attacks can also come from any direction and from a variety of sources – state, non-state, or a combination thereof – in ways that could inflict enormous damage to advanced, networked militaries and societies. Fortunately, the U.S. and Japan maintain a qualitative edge in satellite and computer technology – an advantage we are putting to good use in developing ways to counter threats to the cyber and space domains*."[278] The concern expressed here is barely tempered by the certainty of a technological advantage on the part of the United States and Japan.

In view of the number of speeches given by the Secretaries of Defense, those which speak about the issue of Chinese cyberwarfare are, in the final analysis, relatively few.

Defense relations with China need to take place in a climate of cooperation, and encourage exchanges: "*We also need you to strengthen defense ties with China. China's military is growing and modernizing. We must be vigilant. We must be strong. We must be prepared to confront any challenge. But the key to peace in that region is to develop a*

277 *Air Force Association Convention*, As Delivered by Secretary of Defense Robert M. Gates, National Harbor, MD, Wednesday, September 16, 2009, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1379].
278 *Keio University*, As Delivered by Secretary of Defense Robert M. Gates, Keio University, Tokyo, Japan, Friday, January 14, 2011, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1529].

new era of defense cooperation between our countries – one in which our militaries share security burdens to advance peace in the Asia-Pacific and around the world."[279]

During his visit to Beijing in September 2012, Leon Panetta mentioned the cyberspace issue: "*We've made it very clear that our engagement will continue to be guided by our adherence to a set of basic principles, including the following: one, free and open commerce; two, a just international order that emphasizes the rights and responsibilities of nations and the fidelity to the rule of law; three, open access by all to the shared domains of sea and air and space and cyberspace; and, lastly, resolving disputes peacefully, without coercion or the use of force.*"[280]

In a speech delivered in New York in 2012, Leon Panetta pointed to the United States' direct competitors in cyberspace, whose strategies lend legitimacy to the process of reinforcing America's cyberdefense resources: "*Our most important investment is in skilled cyber-warriors needed to conduct operations in cyberspace. Just as DoD developed the world's finest counterterrorism force over the past decade, we need to build and maintain the finest cyber force and operations. We're recruiting, we're training, we're retaining the best and the brightest in order to stay ahead of other nations. It's no secret that Russia and China have advanced cyber capabilities. Iran has also undertaken a concerted effort*

279 *U.S. Naval Academy Commencement*, As Delivered by Secretary of Defense Leon E. Panetta, Annapolis, MD, Tuesday May 29, 2012, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1679].
280 *PLA Engineering Academy of Armored Forces,* As Delivered by Secretary of Defense Leon E. Panetta, Beijing, China, Wednesday, September 19, 2012, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1723].

to use cyberspace to its advantage."[281] In the same section, two types of threats are mentioned: terrorism, and the rise in power of the states of China, Russia and Iran. Leon Panetta identifies two major risks: that of the rise in capability, and that of the opacity, which could give rise to possible misunderstandings, incomprehension, doubts, and interpretation errors: "*I recently met with our Chinese military counterparts just a few weeks ago. As I mentioned earlier, China is rapidly growing its cyber capabilities. In my visit to Beijing, I underscored the need to increase communication and transparency with each other so that we could avoid a misunderstanding or a miscalculation in cyberspace. This is in the interest of the United States, but it's also in the interest of China*."[282]

China and cyberwarfare constitute a threat to the collective security of Europe and the United States, said Chuck Hagel in 2013, because they contribute to the global threat: "*The foundation of our collective security relationship with Europe has always been cooperation against common threats. Throughout most of the 20th century, these common threats were concentrated in and around Europe. But today, the most persistent and pressing security challenges to Europe and the United States are global. They emanate from political instability and violent extremism in the Middle East and North Africa, dangerous non-state actors, rogue nations, such as North Korea, cyber-warfare, demographic changes, economic disparity, poverty and hunger. And as we confront these threats, nations such as China and Russia are rapidly modernizing their militaries and global defense industries,*

281 "*Defending the Nation from Cyber-Attack*" (Business Executives for National Security), As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728].

282 "*Defending the Nation from Cyber-Attack*" (Business Executives for National Security), As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728].

challenging our technological edge in defense partnerships around the world."[283] On the other hand, China has to play an active role in security – particularly in Asia: "*No security architecture in Southeast Asia can succeed without the active involvement and participation of the two large emerging powers that border this region, China and India*."[284]

Cooperation with China has now been engaged in matters of Cybersecurity: "*As part of our rebalance, the United States is committed to pursuing a positive and constructive relationship with China. We have very open discussions with China, including a productive visit last week by my counterpart, Defense Minister General Chang, whom I hosted at the Pentagon. He and I agreed that we must increase our cooperation and our mutual understanding, including through more defense exercises and the recently established U.S.-China Cyber Working Group. And we continue to encourage China to work toward greater transparency*."[285]

The DoD accuses China of cyber-attacks, whilst calling for greater cooperation and dialog on the issue: "*We are also clear-eyed about the challenges in cyber. The United States has expressed our concerns about the growing threat of cyber intrusions, some of which appear to be tied to the Chinese government and military. As the world's two largest economies, the U.S. and China have many areas of common interest and concern, and the establishment of a cyber*

283 *Munich Security Conference,* As Delivered by Secretary of Defense Chuck Hagel, Munich, Germany, Saturday, February 01, 2014, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1828].
284 *Malaysian Institute of Defense and Security,* As Delivered by Secretary of Defense Chuck Hagel, Malaysian Ministry of Defense, Kuala Lumpur, Malaysia, Sunday August 25 2013, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1799].
285 *Malaysian Institute of Defense and Security,* As Delivered by Secretary of Defense Chuck Hagel, Malaysian Ministry of Defense, Kuala Lumpur, Malaysia, Sunday August 25 2013, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1799].

working group is a positive step in fostering U.S.-China dialogue on cyber. We are determined to work more vigorously with China and other partners to establish international norms of responsible behavior in cyberspace."[286]

In June 2014, Chuck Hagel delivered a speech at the National Defense University in Beijing. In it, he made mention of cyberspace several times:

– The economies of the great nations are mutually interdependent, but in order to prosper they require stability – particularly at a regional level. However, the threats arising in cyberspace are among the destabilizing factors liable to hamper economic expansion. In this respect, China and the United States have a shared interest (peace for/because of the economy): "*As our economic interdependence grows, we have an opportunity to expand the prosperity this region has enjoyed for decades. To preserve the stable regional security environment that has enabled this historic economic expansion, the United States and China have a very big responsibility to address new, enduring regional security challenges alongside all the partners of the Asia-Pacific. We face North Korea's continued dangerous provocations, its nuclear program, and its missile tests; ongoing land and maritime disputes; threats arising from climate change, natural disasters, and pandemic disease; the proliferation of dangerous weapons; and the growing threat of disruption in space and cyberspace*."[287]

– The United States wishes to decry Chinese practices (cyber-espionage) and also to find a solution; the Americans

286 *International Institute for Strategic Studies (Shangri-La Dialogue),* As Delivered by Secretary of Defense Chuck Hagel, Singapore, Saturday June 01 2013, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1785].

287 *PLA National Defense University,*As Delivered by Secretary of Defense Chuck Hagel, Beijing, China, Tuesday April 08 2014, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1838].

want greater communication and less opacity, and call on China to communicate about its cyber strategies, as the US does: "*Openness and two-way communication is especially important in the area of strategic and emerging capabilities, and in managing regional security challenges. It is why we seek to resume a U.S.-China nuclear policy and strategy dialogue. It is also why, through our Cyber Working Group, the United States has been forthright in our concerns about Chinese use of networks to perpetrate commercial espionage and intellectual property theft. We've also made efforts to be more open about our cyber capabilities, including our approach of restraint. Those efforts recently took a major step forward when the Department of Defense, for the first time ever, provided to representatives of the Chinese government a briefing on DoD's doctrine governing the use of its cyber capabilities. We've urged China to do the same*."[288]

– The United States will defend the principle of freedom of access to cyberspace: "*Here in the Asia-Pacific and around the world, the United States believes in maintaining a stable, rules-based order built on free and open access to sea lanes and air space, and now, cyberspace*". The "freedom", of course, relates to economic and security interests, but also to conflicting values (America's desire to impose liberal democratic values on the whole of the world).

8.2.3. *Prospective analyses conducted by the National Intelligence Council*

The "Global Trends 2010" report[289], published in November 1997, predicts that powerful states will lose some

288 *PLA National Defense University,* As Delivered by Secretary of Defense Chuck Hagel, Beijing, China, Tuesday April 08 2014, [http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1838].

289 National Intelligence Council, *Global Trends 2010*, Washington, November 1997, [http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends/global-trends-2010].

of their prerogatives because of the expansion of information technologies throughout the world: "*governments* whose states are relatively immune from poverty and political instability will still *find that they are losing control of significant parts of their national agendas due to the globalization and expansion of the economy, and the continuing revolution in information technology*". The report also holds that "*information technologies will continue to be the hallmarks of the revolution in military affairs*". These considerations about ICTs do not include the prefix particle "cyber". Nor do they associate China with ICT issues. The authors of the report do not envisage China, in the short or medium term, becoming a genuine military power, as they imagine this process would be disrupted by the country's internal problems (managing growth, urbanization, energy and food requirements, etc.).

"Global Trends 2015"[290], published in December 2000, introduces the issue of the cyber threat – one of a variety of transnational problems which the United States is likely to have to face by 2015. The cyber threat is all the greater because American society is so heavily dependent on computer networks. Thus, this theme – a cyber threat posed to the critical infrastructures, and therefore to the whole of society – was already on the radar nearly 15 years ago: "*Increasing reliance on computer networks is making critical US infrastructures more attractive as targets. Computer network operations today offer new options for attacking the United States within its traditional continental sanctuary—potentially anonymously and with selective effects. Nevertheless, we do not know how quickly or effectively such adversaries as terrorists or disaffected states will develop the tradecraft to use cyberwarfare tools and technology, or, in*

290 National Intelligence Council, *Global Trends 2015, A Dialogue about the Future with nongovernment experts,* Washington, December 2000, 98 pages, [http://www.dni.gov/files/documents/Global%20Trends_2015%20Report.pdf].

fact, whether cyberwarfare will ever evolve into a decisive combat arm". China is not associated with the issue of a cyber threat. It is, however, associated with the threat of Weapons of Mass Destruction: "*Short- and medium-range ballistic missiles, particularly if armed with WMD, already pose a significant threat overseas to US interests, military forces, and allies. By 2015, the United States, barring major political changes in these countries, will face ICBM threats from North Korea, probably from Iran, and possibly from Iraq, in addition to long-standing threats from Russia and China.*"

The report "Global Trends 2020, Mapping the Global Future"[291], published in 2004, tackles the question of cyber-warfare, which is the title of one of its chapters.[292] Major cyber-attacks are likely to be attributable to terrorism. ("*Bioterrorism appears particularly suited to the smaller, better-in found groups. We also expect that terrorists will attempt cyber-attacks to disrupt critical information networks and, even more likely, to cause physical damage to information systems*") rather than to a State such as China. When the report speaks of China, it is not to describe it as presenting a cyber threat, but rather to highlight its vulnerability to economic instability and its progress in terms of knowledge production (China produces more graduates than any other major power – a process which will undoubtedly help it to eventually overcome its technological out datedness), and its capacity to create a regional security order in case the Americans withdraw.

291 National Intelligence Council, *Global Trends 2020, Mapping the Global Future*, December 2004, Washington, 123 pages, [http://www.dni.gov/files/documents/Global%20Trends_Mapping%20the%20Global%20Future%202020%20Project.pdf].
292 See page 97 of the report.

In the view of the authors of the "Global Trends 2025" report[293], published in 2008, America is likely to lose some of its advantage in terms of power, although its power will remain quite considerable. Cyberspace is one of the factors in the closing of the gap, which will have consequences for the exercising of American power: "*growing use of cyberwarfare attacks increasingly will constrict US freedom of action*". The report defines "cyber" both as one of the non-military aspects of confrontation between states ("*Non-military means of warfare, such as cyber, economic, resource, psychological, and information-based forms of conflict will become more prevalent in conflicts over the next two decades*") and as a tool to help circumvent American strength ("*Cyber and sabotage attacks on critical US economic, energy, and transportation infrastructures might be viewed by some adversaries as a way to circumvent US strengths on the battlefield and attack directly US interests at home*"). The mention of cyberspace (only 4 times) is not associated with the mention of China (154 references in the text). In this document, the Chinese cyber threat is not amongst the scenarios for the evolution of the international scene.

"Global Trends 2030"[294], published in 2012, makes more mention of the "cyber" notion (36 references). In relation to cyber, the report evokes:

– the new capabilities provided to individuals and non-state actors ("*individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence—*

293 National Intelligence Council, *Global Trends 2025, A transformed world*, November 2008, Washington, 120 pages, [http://www.aicpa.org/research/cpahorizons2025/globalforces/downloadabledocuments/globaltrends.pdf].

294 National Intelligence Council, *Global Trends 2030, Alternative Worlds*, 166 pages, 2012, Washington, [http://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf].

a capability formerly the monopoly of states") which will benefit from facilitated access to a whole new range of weapons. Terrorists could profitably exploit these new technologies and those who have mastery of them: "*With more widespread access to lethal and disruptive technologies, individuals who are experts in such niche areas as cyber systems might sell their services to the highest bidder, including terrorists who would focus less on causing mass casualties and more on creating widespread economic and financial disruptions;*"

– "cyber" technologies are amongst the four forms of technology which will shape the world's economic, social and military future. In particular, the report identifies data managing as a source of power (as the world moves into the Age of Big Data). However, the fear of an Orwellian order could drive societies to rein their governments in, with relation to their exploitation of big data;

– the risks of cyber-attacks by non-state actors rank among the major destabilizing factors;

– the report introduces notions which are absent from the previous reports: cyber weapons, cyber-attacks and cybercrime.[295]

In the various scenarios proposed, the cyber object is not directly correlated with the variable "China". China is presented as one of the potential major factors in destabilizing the international scene: "*China is slated to pass the threshold of US$15,000 per capita purchasing power parity (PPP) in the next five years or so—a level that is often a trigger for democratization. Chinese "soft" power could be dramatically boosted, setting off a wave of democratic movements. Alternatively, many experts believe a democratic China could also become more nationalistic. An economically*

295 See page 67 of the report.

collapsed China would trigger political unrest and shock the global economy". This scenario does not associate China with a cyberthreat.

8.3. Conclusion

Topics	Global Trends 2010 (published in 1997)	Global Trends 2015 (published in 2000)	Global Trends 2020 (published in 2004)	Global Trends 2025 (published in 2008)	Global Trends 2030 (published in 2012)
ICTs lead to a reduction in the power of states; they have a leveling effect; emergence (empowerment of non-state actors, terrorists, individuals)	O			O	O
ICTs: of crucial importance in the RMA[296]	O				
Introduction of the notion of a cyberthreat		O			
Dependence of societies on computer networks: source of vulnerability		O			
China is unlikely to become a military power in the short term	O				
China: nuclear threat		O			
China: unstable, fragile society, etc.		O	O		
China: high rate of knowledge production, high-level graduates			O		

296 RMA: Revolution in Military Affairs.

China as a factor in destabilization of the international scene					O
Cyberwarfare			O		
Danger of a massive-scale cyberattack: terrorism			O		
Cyber is not the only technology which is transforming societies					O
Importance of data control					O
If citizens are fearful of an Orwellian order, there is pressure on states to reduce their use of big data					O

Table 8.1. *The topics discussed in the Global Trends reports (regarding Chinaand cyberspace)*

The reports of the National Intelligence Council therefore do not always associate China with "cyber". China is not depicted as being a cyber threat. The authors of the reports prefer to emphasize the uncertainties engendered by the situation in China (what form of growth is taking place, how is the society evolving? etc.), which cause destabilization both within China and on the international scene. Whilst ICTs are at the heart of the issues of reconfiguration of the power balances (empowerment of individuals, non-state actors, terrorism, etc.), and whilst social pressure (because of the fear of an Orwellian world order) could cast doubt on the policies of countries in terms of data control and exploitation, it is also worthy of note that ICTs are not the only factors in the evolution of modern societies. This approach enables us to situate cyber issues within a broader field of problems,

and to view China in the international space as something other than an agent upsetting order and security strategy because of its ambitions in cyberspace.

Topics relating to China	02	03	04	05	06	07	08	09	10	11	12	13
Concepts												
Information operations	O	O										
Information warfare	O	O							O	O		
Computer network operations				O					O	O	O	O
IO/IW:are strategically important for China	O											
Anti-access strategy	O	O				O						
Local wars under conditions of informationalization				O								
Integrated Network Electronic Warfare				O	O	O	O					
Cyberwarfare								O	O	O	O	O
Cyberespionage											O	O
Information Security Code of Conduct											O	O
Capabilities												
IO capabilities outdated, but in the process of being modernized. Constant development of capabilities		O	O	O	O	O	O	O	O			
Importance of the economic, industrial and R&D relations with foreign actors, helping China to speed up the improvement of its capabilities in the area of ICT, and particularly military IO			O									

Use of reservists to enhance the military's cyberdefense capabilities	O	O			O							
Chinese cyberdefense is operational												O
Strategy, role of ICTs and cyberspace												
Equalizing/leveling nature of the use of cyberspace (facilitates an asymmetrical conflict)	O	O										
Offensive strategy	O	O			O							
Defensive strategy	O	O										
Nationalistic hacking (supported by the State)	O	O										
Cyber = pre-emptive weapon		O										O
Possible range of applications of China's IO/IW capabilities: conflict with Taiwan			O									
Cyber-attacks originating in China are afflicting the United States							O	O	O	O	O	O

Table 8.2. *Chinese Cybersecurity, cyberdefense and cyberspace, according to the DoD's annual report to Congress*

The DoD reports seem to focus on three main areas: the concepts which feed into China's policies and defense strategies; the development of capabilities; and the strategy itself, the role attributed to ICTs and cyberspace.

In terms of concepts, although the notions of IW and IO have remained throughout the period 2002-2013, we can see that a transition takes place around 2005 (when the

discussion is of the notion of Integrated Network Electronic Warfare), and then around 2008 there is a change of vocabulary to "cyber", with discussions about cyberdefense (cyber-warfare, cyber-espionage, etc.). In terms of capabilities, whilst the reports highlighted how outdated the Chinese army was in 2002, all the later reports speak of the constancy of its efforts to develop, which are based on industry, and policies of acquisition of resources from outside the army (reserves and militias). Finally, in 2013, the report states that China's cyberdefense is operational. Whilst the threat lay in the volatile relations between China and Taiwan at the start of the 2000s, from 2008 onwards the United States' main concern demonstrably changes to the cyber-attacks to which it is being subjected. Thus, in the space of 12 years, according to these reports, China seems to have gone from having an armed force "under construction" to having an operational, active and offensive cyberdefense protocol. In this process, 2007-2008 seems to have been a hinge point. However, is this impression actually a reflection of the reality in China, or is it one that has been strategically projected by the Americans?

From the speeches given by the US Secretaries of Defense, we can also see that a transition took place in 2005-2006. From then on, China began making appearances in their speeches. There are two competing themes: one which condemns the opacity of the Chinese discourse, the lack of perspectives and clearly-declared intentions in terms of defense, which gives rise to doubts and concerns, instability which is damaging for the world economy; in parallel to this we see the call for greater exchanges and dialog, because the two nations are not enemies, but in fact have shared responsibilities when it comes to ensuring world stability. The table below clearly demonstrates the emergence of debate about China from the mid-2000s – particularly around 2007-2008, i.e. the period when the DoD reports began to openly condemn the cyber-attacks directed at America. Thus, just as we speak of "post-9/11" in reference to

the turning point in the area of terrorism, in the debates about China and cyberspace in general, we can speak of the "post-2007" period.

Topics	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
The USA is concerned about China's progression: its place in the world, and its ambitions												O											
The USA criticizes the opacity of the Chinese discourse														O	O								
Uncertainties regarding the aims of the Chinese military developments														O									
China is not an enemy of the United States. Cooperation is needed, and is taking place																				O	O	O	
China is a threat because of its developments of military capabilities. Threat to collective security																	O	O				O	
Chinese anti-access strategy																		O		O			
China = a competitor for the USA in cyberspace																					O		
The economies of the great nations are mutually interdependent. There is a need for stability. Cyberspace and Chinese practices = risk of destabilization																							O

Table 8.3. *Themes in discourse on China in the DoD Annual Reports*

General Conclusion

The scenario of a Chinese cyber-threat feeds into the discourse held in the circles of security and defense in many countries. It intersects with the scenario of the threat against critical infrastructures. For example, Congressman Mike Rogers, Chairman of the House Permanent Select Committee on Intelligence and a former FBI agent, is the proponent of a law bill entitled "*The Cyber Intelligence Sharing and Protection Act*"[1], the aim of which is to "*facilitate information sharing, interaction, and collaboration among and between federal, state, local, tribal, and territorial governments, cybersecurity providers, and self-protected entities.*"[2] He supports this project because of the need to protect America from the threat of cyber-attacks from China, Russia and Iran against the country's infrastructures. Others maintain that China is conducting massive-scale cyber-espionage operations. According to the US Office of the National Counter Intelligence Executive (ONCIX): "*America's annual costs due to cyber espionage could be as*

Conclusion written by Daniel VENTRE.

1 H.R.624 – *Cyber Intelligence Sharing and Protection Act*, [http://beta.congress.gov/bill/113th-congress/house-bill/624].

2 Summary: H.R.624 – 113th Congress (2013-2014), [http://beta.congress.gov/bill/113th-congress/house-bill/624].

high as $400 billion a year [...] *Chinese actors are the world's most active and persistent perpetrators of economic espionage.*"[3]

The topics and arguments interweave with one another to form the scenario presented in the graph below.

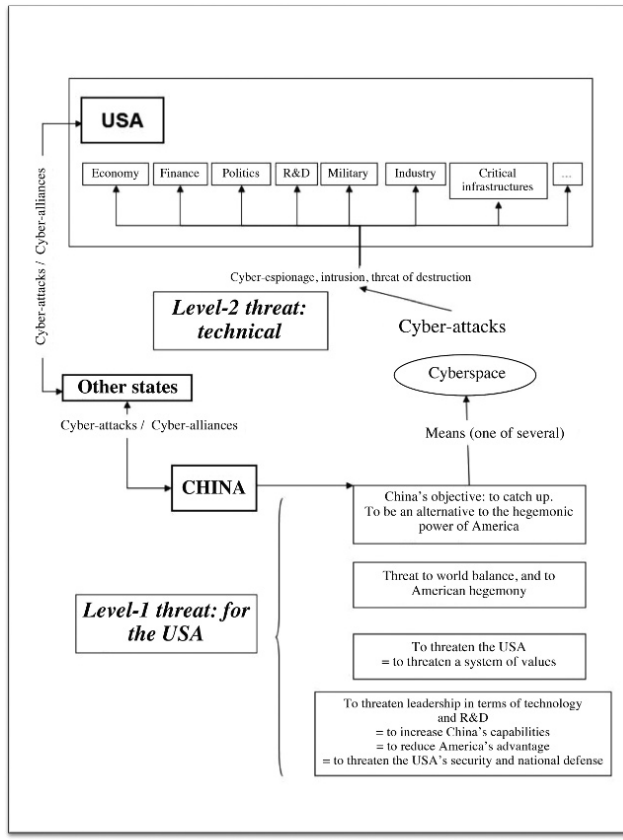


Figure C.1. *The scenarios (and their components) of the Chinese cyber-threat*

3 Cited in: Lu Jinghua, *China's Cyber Threat: Real or Imaginary?*, June 7, 2013, [http://www.chinausfocus.com/peace-security/chinas-cyber-threat-real-or-imaginary/].

Yet to what extent are the argument of the "Chinese cyber-threat", or even simply China's cyberspace policy and strategy, taken into account in the definition of the cybersecurity and cyberdefense strategies for other nations, be they large or small, near to or far from China?

An initial indication can be found in the formulations of the national cyber strategies published in recent years.

Cyber strategy document	Country	Year	Reference to China?	Terms of reference to China, if applicable
Cybersecurity Strategy[4]	Australia	2009	No	
Austrian Cybersecurity Strategy[5]	Austria	2013	No	
Canada's cybersecurity strategy[6]	Canada	2010	No	
Cybersecurity Strategy of Czech Republic for the 2011-2015 Period (2011)[7]	Czech Republic	2011	No	
Cybersecurity Strategy[8]	Estonia	2008	No	

4 Cybersecurity Strategy, Australian Government, 2009, 38 pages, [http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf].
5 Austrian Cybersecurity Strategy, Federal Chancellery of the Republic of Austria, 2013, 25 pages, [https://www.bka.gv.at/DocView.axd?CobId=50999].
6 Canada's Cybersecurity Strategy, Government of Canada, 17 pages, 2010, [http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf].
7 Cybersecurity Strategy of Czech Republic for the 2011-2015 Period, 2011, 10 pages, [http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF].
8 Cybersecurity Strategy, Ministry of Defence, Tallinn, 2008, 36 pages, [http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf].

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[9]	EU	2013	No	
Finland's Cybersecurity Strategy[10]	Finland	2013	No	
Defense et sécurité des systèmes d'information. Stratégie de la France [11]	France	2011	No	
Cybersecurity Strategy for Germany[12]	Germany	2011	No	
National Cybersecurity Strategy[13]	Hungary	2013	No	
National Cyber security Policy[14]	India	2013	No	

9 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, 7 February 2013, 20 pages, [http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667].

10 Finland's Cybersecurity Strategy, Government Resolution 24.1.2013, 2013, 44 pages, [http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf].

11 ANSSI, Défense et sécurité des systèmes d'information. Stratégie de la France, February 2011, 24 pages, [http://www.ssi.gouv.fr/IMG/pdf/2011-02-5_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf].

12 Strategy for Germany, Federal Ministry of the Interior, February 2011, 20 pages, [http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-hemen/css_engl_download.pdf?__blob=publicationFile].

13 National Cybersecurity Strategy, Hungary, 7 pages, March 2013, [http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx].

14 National Cybersecurity Policy, India, July 2013, 10 pages, [http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf].

National Strategic Framework for Cyberspace Security[15]	Italy	2013	No	
International Strategy on Cybersecurity – j-Initiative for Cybersecurity[16]	Japan	2013	No	
Cybersecurity Strategy[17]	Japan	2013	No	
Information Security Strategy for protecting the nation[18]	Japan	2010	No	
National Cybersecurity Strategy and Master Plan[19]	Kenya	2013	No	

15 National Strategic Framework for Cyberspace Security, Presidency of the Council of Ministers, Italy, December 2013, 48 pages, [http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf].

16 International Strategy on Cybersecurity - j-Initiative for Cybersecurity, Information Security Policy Council, 2 October 2013, 17 pages, [http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf].

17 Cybersecurity Strategy, Information Security Policy Council, 10 June 2013, 55 pages, [http://www.nisc.go.jp/active/kihon/pdf/cybersecurity strategy-en.pdf].

18 Information Security Strategy for protecting the nation, Information Security Policy Council, Japan, May 2010, 20 pages, [http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf].

19 National Cybersecurity Strategy and Master Plan, Ministry of Information and Communication, February 2013, [http://www.information.go.ke/Downloads/ICT_MASTER_PLAN_2017.pdf].

Programme for the development of electronic information security (cybersecurity) for 2011-2019[20]	Lithuania	2011	No	
National strategy on cybersecurity[21]	Luxembourg	2011	No	
The NATO Policy on Cyberdefence[22]	NATO	2011	No	
The National Cybersecurity Strategy 2[23]	Netherlands	2013	No	
The National Cybersecurity Strategy[24]	Netherlands	2011	No	
The Defence Cyber Strategy [25]	Netherlands	2012	No	

20 Programme for the development of electronic information security (cybersecurity) for 2011-2019, Government of the Republic of Lithuania, June 2011, 17 pages, [http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf].

21 Stratégie nationale en matière de cyber sécurité, Ministère d'Etat, Le Gouvernement du Grand-Duché de Luxembourg, 10 pages, 2011, [http://www.mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_12 2011.pdf].

22 The NATO Policy on Cyberdefence, Brussels, 2011, 2 pages, [http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence-fr.pdf].

23 The National Cybersecurity Strategy 2, National Coordinator for Security and Counterterrorism, 36 pages, 2013, [http://english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf].

24 The National Cybersecurity Strategy, Ministry of Security and Justice, Netherlands, 16 pages, June 2011.

25 Ministry of Defence, The Defence Cyber Strategy, Netherlands, September 2012, 20 pages, [http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf]

New Zealand Cybersecurity Strategy[26]	New Zealand	2011	No	
Cybersecurity Strategy for Norway[27]	Norway	2013	No	
Cybersecurity Strategy and the National Action Plan on implementation of the national cybersecurity [28]	Romania	2011	No	
The Information Security Doctrine of the Russian Federation[29]	Russia	2000	No	
National Strategy for Information security in the Slovak Republic[30]	Slovakia	2008	No	
Cybersecurity policy of South Africa[31]	South Africa	2010	No	

26 New Zealand's Cybersecurity Strategy, New Zealand Government, 2011, 16 pages, [http://www.dpmc.govt.nz/sites/all/files/publications/nz-cybersecurity-strategy-june-2011_0.pdf].

27 Cybersecurity Strategy for Norway, Norwegian Ministries, 32 pages, April 2013, [http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf].

28 Cybersecurity Strategy and the National Action Plan on implementation of the national cybersecurity, 2013, 17 pages, [http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf].

29 The Information Security Doctrine of the Russian Federation, September 2000, [http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument].

30 National Strategy for Information security in the Slovak Republic, 2008, 20 pages, [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf].

31 Cybersecurity policy of South Africa, May 2011, 33 pages, [http://www.cyanre.co.za/national-cybersecurity-policy.pdf].

National Cybersecurity Strategy	South Korea	2011		
Defense White Paper[32]	South Korea	2010	Yes	About the regional security structure (p. 14): "China and Russia, too, have been strengthening their strategic partnership … China and Japan are expanding their military exchanges through mutual visits of high-ranking officials and navy vessels." This analysis focuses on relations in terms of defense in general, rather than on the cyber dimension in particular. The chapter on cyberdefense (pp. 158–165) does not mention China.

32 Defense White Paper, Ministry of National Defense, South Korea, 2010, 440 pages, [http://www.nti.org/media/pdfs/2010WhitePaperAll_eng.pdf?_=1340662780].

Estrategia de Ciberseguridad Nacional[33]	Spain	2013	No	
National strategy for Switzerland's protection against cyber risks[34]	Switzerland	2012	No	
National Cybersecurity Strategy[35]	Trinidad and Tobago	2012	No	
National Cybersecurity Strategy and 2013-2014 Action Plan[36]	Turkey	2013	No	
National Information Security Strategy[37]	Uganda	2013	No	
The UK Cybersecurity Strategy[38]	United Kingdom	2011	No	

33 Estrategia de Ciberseguridad Nacional, Presidencia del Gobierno, Departamento de Seguridad Nacional, 55 pages, 2013, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf].

34 National strategy for Switzerland's protection against cyber risks, Federal Department of Defence, Civil Protection and Sport DDPS, 27 June 2012, 42 pages, [http://www.isb.admin.ch/themen/01709/01710/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCEeX9,fGym162epYbg2c_JjKbNoKSn6A--&t=.pdf].

35 National Cybersecurity Strategy, Government of the Republic of Trinidad & Tobago, December 2012, 29 pages, [http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf]

36 National Cybersecurity Strategy and 2013-2014 Action Plan, Republic of Turkey, Ministry of Transport, Maritime Affairs and Communications, 47 pages, 2013, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/TUR_NCSS.pdf].

37 National Information Security Strategy, Republic of Uganda, Ministry of Information and Communications Technology, March 2011, 55 pages, [http://www.nita.go.ug/uploads/NISS.pdf].

38 Cabinet Office, The UK Cybersecurity Strategy, November 2011, 43 pages, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf].

Cybersecurity Strategy of the United Kingdom[39]	United Kingdom	2009	No	
The National Cybersecurity Strategy[40]	United Kingdom	2013	Yes	"The UK has also agreed to hold a formal dialogue on cyber with China"
International Strategy for Cyberspace[41]	United States	2011	No	
National Strategy to Secure Cyberspace[42]	United States	2003	Yes	About IPv6: "China is also considering early adoption of the protocol." (p. 30)
Department of Defense Strategy for Operating in Cyberspace[43]. Document influenced by the NMS-CO of 2006.	United States	2011	No	

Table C.1. *National strategies for cybersecurity*

39 Cybersecurity Strategy of the United Kingdom, Cabinet Office, June 2009, 32 pages, [http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf].

40 The National Cybersecurity Strategy, The Cabinet Office, December 2013, 15 pages, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf].

41 International Strategy for Cyberspace, The White House, Washington, May 2011, 30 pages, [http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf].

42 White House, The National Strategy to Secure Cyberspace, United States, February 2003, 76 pages [https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf]

43 Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, United States, July 2011, 19 pages, [http://www.defense.gov/news/d20110714cyber.pdf].

Only 3 documents in this corpus actually make reference to China: one to point out the IPv6 is being adopted by China; the second to mention the establishment of, or willingness for, dialog with China over cybersecurity issues; and the third to speak of China's increasingly close military ties with third parties, although the cyber issue is not mentioned. Perhaps the writers of the various national strategies are conscious of the threats posed by China, but these national strategies are primarily formulated with the aim of overall protection, against all types of attacks. The "problem" of China, which is so apparent in the discourse in the media, from political and industrial actors, is not mentioned in the official documents. Other variables have recently come into play to constrain these strategic stances. The crisis of trust which has taken hold in the international community, in the wake of Edward Snowden's revelations about American cyber-espionage practices (America's allies were not at all appreciative of being targeted by such measures), is liable to impact numerous political and strategic choices for cyberspace – at least as much as considerations about China's policies and practices.

List of Authors

Dean CHENG
Asia Studies Center
The Heritage Foundation
Washington DC
USA

Alan CHONG
S. Rajaratnam School of
International Studies
Singapore

Alice EKMAN
French Institute of
International Relations (Ifri)
Paris
France

Thomas FLICHY DE LA
NEUVILLE
Saint-Cyr Military Academy
Guer
France

Xu LONGDI
China Institute of
International Studies (CIIS)
Beijing
China

Cherian SAMUEL
Strategic Technologies
Centre
Institute for Defence Studies
and Analysis
New Delhi
India

Daniel VENTRE
CESDIP
CNRS/University of
Versailles/Ministry of Justice
France

Index

J, K, L

M

N, O, P