Safeguarding Defense Technology, Enabling Commerce

Safeguarding Defense Technology, Enabling Commerce

A New Balance in the New Economy

Seth Cropsey

The AEI Press
Publisher for the American Enterprise Institute

WASHINGTON, D.C.
2001

Available in the United States from the AEI Press, c/o Publisher Resources Inc., 1224 Heil Quaker Blvd., P.O. Box 7001, La Vergne, TN 37086-7001. To order, call 1-800-937-5557. Distributed outside the United States by arrangement with Eurospan, 3 Henrietta Street, London WC2E 8LU, England.

ISBN 0-8447-7158-9

1 3 5 7 9 10 8 6 4 2

The AEI Press
Publisher for the American Enterprise Institute
1150 17th Street, N.W.
Washington, D.C. 20036

Printed in the United States of America

Dedicated to the memory of Al Bernstein
1939–2001
Scholar ✯ Patriot ✯ Friend

Contents

Foreword

More than ten years after the symbolic end of the cold war—the fall of the Berlin Wall in 1989—the United States and its allies are still sorting out which foreign policy issues have become obsolete and which endure. With American products at the leading edge of technology's advancing wave, the questions raised by exports of sensitive technology have never been more important. Yet we continue to address the issues surrounding the control of high-tech exports with little regard to the differences in the pace of technological change and the extent of globalization that separate 2001 and 1989. Policies that were invaluable during the cold war have been continued as a result of inertia but to no useful end. This is a mistake. Radical change is needed.

It is, however, important to recall how those policies worked and what ends they served; the principle of how to think about export controls does not change.

Cold War Policies Vindicated

One day, early in 1981, after I arrived at the Department of Defense, an intelligence officer came to see me with an extraordinary document. It was based on reporting from a Soviet official, cooperating with American intelligence, who shared with us detailed knowledge of the massive Soviet

program then underway to acquire Western technology in order to improve Soviet military and intelligence systems.

The document identified over 5,000 Soviet military programs that depended on a continuous infusion of Western technology, including the Soviets' key intercontinental ballistic missile programs, their key aircraft programs, their key missile programs of all kinds. Beautifully organized, this extraordinary road map identified each Soviet military program, the technology needed to accomplish it, the vendors in the United States and elsewhere, and the Soviet organizations responsible for assuring the flow of the appropriate equipment.

Consider the case of the Soviet SS-20, an intermediate-range ballistic missile that was very important in those days. It was the spearhead of the Warsaw Pact's effort to divide the Atlantic alliance by threatening Western Europe with nuclear devastation. We learned that the SS-20 program in particular depended heavily on Western technology for everything from the isostatic presses that crafted the body of the missile, through the engine technology, the nozzle technology, the ablative material for the warheads, and the like.

In short, the Soviets were engaged in a comprehensive effort to reach into the technological resources of the West in order to improve their own military capability. Recognizing that the security of this nation and its allies depended on cutting off the flow of Western technology to these critical Soviet military programs, we acted. First, Deputy Secretary of Defense Frank Carlucci decided to shift the responsibility within the Department of Defense for the export control process to my office in order to rationalize organizational purpose. I recall distinctly what he said: "I'm giving you this responsibility, and the reason is that I think you're going to take it seriously, and we have an urgent problem."

My objective was to stop the technology's transfer. The people who had previously been in charge had, at best, a divided mission, since one of their other purposes was the development of technology. Because they were close to the technological community—as one would expect and as, indeed, was natural and necessary—their enthusiasm for effective controls was limited, to say the least.

We put together a new organization to superintend the export of advanced technology. The existing system for processing export licenses was primitive and did not produce timely, consistent decisions. These flaws were not a result of trying to prevent sensitive technology from reaching the hands of the Soviet Union, but stemmed from the way the program had been administered. There were no computers, for example. Things were being done in hard copy, and it was an endless process. Indeed, those who complained about delays at the time were right to do so.

We put in place a new system and began to expedite approvals. By the time we left office, the system was far more efficient.

The Soviet official mentioned above who had passed us the information about his country's procurement of Western technology was ultimately discovered—and executed. This was unfortunate proof that we were right to treat the information he passed along with extreme sensitivity. In fact, because he was in jeopardy as a source of valuable information, we had been unable to explain in public, as convincingly as we would have liked, why we resorted to what some people regarded as draconian measures to restrict exports.

But without exception, former Soviet defense industry officials and Americans who visited Soviet defense installations now insist that American technology was very important to the Soviets.

I was in Russia not long ago and was surprised to be escorted around what I believe is the largest flight-test

facility in the world. There, not far from Moscow, I was shown a military aircraft currently under development; I was permitted to see whatever I wanted in the way of their laboratories and their test facilities.

The Russians were so open because they are looking for marketing partners for their latest MiG aircraft, and other equipment. They freely volunteer the importance of Western technology during the cold war, which means that in the 1980s we were right to take the steps that we did. We did not perform perfectly; there was excessive zeal on occasion. But I believe history has already shown we were right to attempt what we did.

What Do We Do Now?

Today our problem is different. The United States no longer faces an enemy that, like the Soviet Union, is building a military establishment of enormous proportions and directly threatening the United States and our friends and allies. We no longer confront the daily prospect that a vitally important, high-powered oscilloscope, or a piece of measuring equipment, or a test-range radar may fall into the hands of the enemy with grave consequences.

There are countries whose military capabilities we must watch carefully and toward which it is wise to control our exports—where it is possible. There remain equipment and technology of great military importance that should be kept out of the hands of potential adversaries, if a way to accomplish this can be found. But we need an approach quite different from what was called for during the cold war.

For example, it makes no sense to try to control the export of equipment that is generally available around the world. This is particularly true in an area of great importance to the United States, both commercially and militarily: computing capability.

Because computing power is easy to obtain from numerous sources, we cannot realistically hope to control it. Any policy whose objective is doomed from the beginning is useless to promulgate. The general and increasing availability of computers around the world sentences efforts to control them to such a fate.

But a class of computers does exist that is not generally available, and these machines are disproportionately represented in military research and development, including such critical military applications as modeling the effects of nuclear weapons. This is a small category of equipment, but even here, attempts at control that use the traditional licensing process are limited by developments like parallel processing, in which computers are linked together to produce additive powers of processing.

Among our friends and allies, the best protection for these powerful machines is vigilance applied case by case. Keeping these and similar computers out of potentially dangerous hands should not depend on an export licensing process. Instead, we should employ more conventional law enforcement efforts that aim at understanding who the consumers are for particular kinds of equipment, and what adverse military consequences are likely to follow from exporting such equipment. We should try to deal with these issues in a variety of imaginative ways, including some that we do not normally consider a part of the export control process.

For example, we ought to conduct "sting" operations almost continuously. Those who hope to obtain highly sensitive equipment which they would not otherwise be permitted to acquire will then be in constant doubt whether they are dealing with someone they can trust, or with a law enforcement operation.

Using uncertainty in this way to put an enemy like Saddam Hussein off balance is a significant accomplishment.

The positive effect applies just as surely to our allies, many of whom are often more generous—and more careless—than we are about selling sensitive technology to rogue states like Iran and Iraq. A good job of law enforcement on our part will also keep them alert. At the very least, sting operations that expose dubious transactions and trace them back to companies in friendly states are an embarrassment to the incautious.

While it is impossible to control every potential technology export, many unconventional things can be done to disrupt rogue states' most egregious misappropriation of technology for military purposes. But we will have to focus controls much more narrowly and selectively.

This is not, however, to repeat the old cliché that we should have "fewer barriers but higher barriers," a cliché as notoriously long on self-interest as it is short on substance. The United States has always tried to control more than we could—and thus should—control. But those who have made the fewer-but-higher-barriers argument were usually aiming not to raise the height of the barriers but only to reduce their scope.

By contrast, I argue that we should focus not on what is being exported, but rather on who is doing the importing and for what purpose. This approach will yield unconventional and thus better methods of control than burdening our entire export industry with regulations that are often unfathomable and poorly administered.

Nowhere is this more obvious than in the category of computing power, whose exponentially increasing power and matching availability make the very attempt to license computers a fool's errand.

The more I look at American military forces today and at the security challenges we face in the future, the more convinced I am that we depend and will continue to depend on the success with which we develop technology for military

purposes. We must, then, continue to foster the improvement of civilian technologies that also have military benefits.

But the real engine of technological growth in the United States and the world today is not the military establishment. It is not the Defense Department budget. It is, rather, in the civilian sector. It is the growing number of people logging onto the Internet and demanding faster communication. It is people looking for sensors that will control automotive performance. It is, in short, the search for the kinds of cheap and rapid data processing that will permit us to operate with great precision in many ways, including militarily.

An Effective Military Requires New Technologies

If America is to maintain an effective military force, that military force must reflect what is referred to as the revolution in military affairs. Put simply, we are now developing technologies that permit us, for the first time, to hit the overwhelming majority of targets at which we aim.

That may seem like a rather basic consideration for the military, but in human history to date, most of the weapons launched, most of the bullets fired, and most of the shells lobbed at the enemy have missed the target. And when you miss the target most of the time, you need a very large military force.

With the capability to hit most of the targets most of the time, a small military force can accomplish large military objectives. This nation will only be able to bring our influence to bear around the world if we incorporate technology that permits American forces to hit the target most of the time. By a fortunate coincidence, the same technologies that permit quantum leaps in accuracy also tend to offer an opportunity to hit the target from beyond the lethal range of the enemy.

But this revolutionary capability will elude us if we hinder technological growth and development. We should all

be quite reluctant to encumber industry except in those instances that provide a clear return for our national security. Much of the export control scheme that remains in place, the regimen that was appropriate for the cold war, is no longer appropriate. It is time for sweeping change.

In the essay that follows, Seth Cropsey provides a blueprint to guide policymakers who will be responsible for bringing our export controls into line with the new circumstances we face.

RICHARD PERLE
American Enterprise Institute

1
Introduction

Ensuring a country's security by denying its adversaries critical military technology is not a modern innovation. In the seventh century A.D., the Byzantine emperor Constantine IV repelled invading Arab fleets with a secret compound called Greek fire, which would explode upon contact with the enemy's wooden vessels and burst into flames that water failed to extinguish and may have fanned. Today, Greek fire is believed to have been based on phosphorus, but the formula was held so closely that the exact composition is still not known for certain. The care with which that secret was kept is one indication of its military importance. Another is the unrelenting effort by other nations to obtain the key.

The Byzantine Empire was the trading center of the eastern Mediterranean, but even as its leaders vigorously plied their commerce, they understood the need to safeguard their winning military technology. "When the barbarians ask for the Greek fire," a later Byzantine emperor warned his son, tell them that "an angel, who brought it to the emperor Constantine, forbade its transfer to other nations, and that those who had dared to do so had been consumed by the fire of heaven upon entering a church."[1]

The finality and awe of that proscription against transferring military technology are not available to us. But the problem it addressed remains: how to keep dangerous

technologies out of potentially hostile hands, without choking the commerce that produces both technology itself and the wealth that contributes to society's well-being. This problem has been exacerbated by the recent explosion of technical knowledge spread across the world's borders through an unprecedented increase in global trade, freer movement of peoples, and the extraordinary growth of the Internet.

In its April 2000 *World Economic Outlook,* the International Monetary Fund cited growing technical exchange when presenting its astonishing estimate that the goods and services produced in the twentieth century exceeded the cumulative human output over all preceding recorded history.[2] From the development of the transistor after World War II, through the microprocessor, computer, satellites, and laser and fiber-optic technologies, mankind has developed an unprecedented capacity to use information to increase economic productivity. By the 1990s, in the words of Federal Reserve Board chairman Alan Greenspan, the "remarkable coming together of technologies that we label IT has allowed us to move beyond efficiency gains in routine manual tasks to achieve new levels of productivity…. As a result, information technologies have begun to alter significantly how we do business and create economic value, often in ways that were not foreseeable even a decade ago."[3]

Indeed, American economic growth has benefited strongly both from technology and from the worldwide prosperity and trade it has fostered. Spurred by free-market policies and exports, the United States has enjoyed almost continuous economic growth since 1983. In that time, the proportion of U.S. gross domestic product accounted for by exports has grown by more than 48 percent.[4] An increasing proportion of those exports involve high technology, as can be seen from a quick glance at statistics reported by trade associations and individual states. Washington state, home

to numerous high-technology companies in the fields of aerospace, biomedicals, software, and telecommunications equipment, projects that one-third of its labor force will hold export-related jobs in 2005. Neighboring Oregon saw its high-tech exports increase from 27 percent of total exports in 1989 to 50 percent seven years later. New Mexico enjoyed a nearly fivefold increase in the dollar value of its high-tech exports from 1994 to 1997. But such growth is not limited to the West and the Sunbelt. The American Electronic Association lists Pennsylvania as the eighth-ranked cyberstate: its high-tech exports climbed 78 percent from 1990 to 1997.[5]

Clearly, Americans have a compelling interest in the continued expansion of an open world economy, as well as in maintaining U.S. competitiveness in world markets. Unfortunately, the same factors that drive economic growth also help spread dangerous weapons. Numerous congressional and other investigations report that U.S. technology, both purchased and stolen, has accelerated the military development of hostile nations and nonstate actors and has enabled them to benefit from our national investments in knowledge as well as our freedom to innovate and trade.

In the post–cold war era, many Americans are tempted to downplay the dangers of this proliferation of weaponry. Our major adversary of forty-five years is gone, and the United States appears to have a significant technological edge over all potential opponents. Even if that were so, however, history shows that aggressive nations can narrow a military gap with great speed. They can develop asymmetric "counter weapons" to neutralize or offset our strengths. We have already seen evidence of what mischief the wicked, armed with the terrible, can cause. In an age of increasingly destructive weaponry, no short-term economic gains can compensate the United States for the loss of its current defense advantage.

China's overt and covert efforts to acquire U.S. technology are perhaps our most important recent failures to guard our military edge. And because of China's large role in weapons proliferation, the same U.S. technology, including weapons of mass destruction, may be transferred to rogue states or terrorists. In 1998, the Rumsfeld Commission (named for its chairman, the former and future Secretary of Defense Donald Rumsfeld) concluded that because of "the illegal acquisition of U.S. designs and equipment and *the relaxation of U.S. export control policies*…the U.S. is today a major, albeit unintentional, contributor to the proliferation of ballistic missiles and associated weapons of mass destruction." (Emphasis added.) The commission specifically noted Russia's and China's roles in the transfer of ballistic missile technology to such flash points as the Middle East and the southeast Asian subcontinent,[6] a warning that was echoed by two subsequent congressional commission reports.[7]

At the same time, efforts to limit the spread of military technology have been complicated by the fact that other developed nations have similar technology and have become a major source for importing countries. Indeed, in many cases, they are an easier source, since few nations have export-control regimens that approach the scope of our own. And with the freer movement of peoples across borders and the explosion of information publicly available on the Internet, more and more technology is available without the need for theft or purchase.

2
The Conflicts Surrounding Export Controls

Can the United States better protect its national security without infringing on the legitimate interests of its citizens who wish to participate in world markets?

Can we set meaningful limits on technology transfer, when technology itself is changing at an unprecedented speed?

How can we cooperate more effectively with other nations to limit the threat of dangerous technologies—and when necessary, how can we operate more effectively alone?

Finally, given the limits on what technologies we can realistically control, are there actions we can take to augment the current export-control regimen?

This American Enterprise Institute study of export controls on defense technology will evaluate the record of export controls from their origin in the cold war to their most recent status under the Clinton administration. It will consider the impact of today's technological revolution, including the key information technologies which underlie that revolution. It will present the insights of a panel of distinguished experts who reviewed the basic elements of American defense superiority in future warfare. And it will conclude with specific policy recommendations for a national security strategy better suited to our new situation.

The possibility that today's ineffectual U.S. policies may unwittingly assist in the proliferation of weapons to potentially hostile states lends urgency to the effort to reestablish effective controls over the transfer of technology. The recommendations that conclude this monograph are a first step.

3
The Cold War Experience

Today's defense export-control regimen developed out of a cold war program begun in the late 1940s that aimed to prevent military transfers to the nascent Soviet empire. By denying technologies to the Soviet bloc, export controls helped shorten the cold war. Yet serious weaknesses in our export regimen allowed Moscow and its satellites to acquire advanced Western technology. The record offers useful lessons for today.

In 1949, the United States and its European allies formed the Coordinating Committee for Multilateral Export Controls (COCOM) to oversee common restrictions on the transfer of Western technology to the Warsaw Pact. Established as a committee under the Paris Consultative Group (which itself died of inertia in the 1950s), COCOM lacked formal legal status and operated initially by unanimous agreement. In keeping with the committee's ad hoc structure, broad theory took a back seat to practical application in its work. Fundamental questions—such as how extensive the restrictions should be, or whether member governments should bind themselves to the committee's decisions through bilateral trade agreements with Moscow—went unasked and unanswered. Nor could the public monitor COCOM developments: the committee's debates, and even its lists of prohibited technologies, were held secret.[8]

In practice, export controls varied according to the temperature of the cold war and a country's policies on free trade. Thus, President Truman, enduring the Soviet roll-up of eastern Europe and then the Korean War, was tough on defense exports; President Eisenhower, who achieved armistice in Korea and had a greater commitment to free trade, permitted somewhat more flexibility. British policy fluctuated similarly.

In cases where other countries could supply an adversary, U.S. export controls would merely be an economic barrier to American companies, not a safeguard of national security. On the other hand, by incrementally expanding the boundaries of what was considered exportable, the Soviets could obtain, and were obtaining, increasingly advanced U.S. military-related equipment.

A classic instance of this dilemma arose in the case of machine tools—the sophisticated manufacturing technologies that remain at issue in U.S.-China trade policy today. In 1960, the Bryant Chucking Grinder Company of Springfield, Vermont, sought to sell to the Soviets the machine tools needed for manufacturing ball races, which are small, corrosion-resistant ball bearings used in aircraft engines, in servomechanisms for fire control, and in gyroscopes for missiles, aircraft, and space vehicles. The Defense Department opposed the sale on security grounds; the Commerce Department favored it, arguing that the Soviets could purchase ball races of equal quality in Europe. In February 1961, after the Senate weighed in against the Commerce position, the Kennedy administration canceled the deal. Yet despite the apparent availability of European ball races, the Soviets continued to seek the Bryant Chucking machinery, which strongly implies that the U.S. technology provided advantages not to be found elsewhere. Thus, eleven years later, amid the thaw following the 1972 Nixon-Brezhnev trade agreement, Bryant Chucking received

an export license to sell 172 grinding machines to Moscow. Just four years after that, the Defense Intelligence Agency reported to Congress that parts ground by the Bryant machines "may now be used in the guidance of Soviet missiles."[9]

As cold war policymakers wrestled with the balance between defense and commercial concerns, they also began dealing with the diffusion of high technology, not only in advanced matériel, machinery, and communications, but also in computer capability. Increasingly, critical technologies had both civilian and military applications that were hard to distinguish in practice and evolving rapidly. The difficulty stemmed not simply from the increasing numbers of potential suppliers, but from the spread of the basic science itself. In the 1960s, the United States proposed sweeping liberalization of COCOM controls on integrated circuits, a key element of the new "dual-use" technology (technology with both civilian and military uses). The circuits' broad availability, Washington contended, meant that efforts to restrict them must fall short of a common sense measure of any export-control regimen: effectiveness.

A Defense Science Board study in the mid-1970s sustained the momentum for limiting COCOM's focus and targeting its efforts only on technologies essential to Soviet military capabilities. The Export Administration Act of 1979 gave bipartisan congressional support to relaxing restrictions on civilian-use products. It fell to a new administration in 1981 to raise serious questions about the export-control regimen's effectiveness in its primary purpose, namely, keeping dangerous Western technologies out of the hands of adversaries.[10]

The Reagan administration recognized that, given increasingly free flows of trade as well as advancing technology, COCOM had not prevented the Communist bloc from importing ostensibly civilian technologies for military

purposes. For instance, trucks used in the invasion of Afghanistan were produced at a Western-built $1.5 billion Kama River truck factory just west of the Urals.[11]

In fact, as the CIA and Defense Department documented, a massive Soviet effort was under way to obtain technological secrets from Western scientific laboratories, universities, and industries. One CIA–Defense Department report estimated that "an average of over 5,000 Soviet military equipment and weapon-system research projects per year in the early 1980s benefited from Western hardware and technical documents."[12] The same study described how Moscow used Western technology and information to redirect about a hundred military programs under design per year.

The report used Soviet sources to show how powerful acoustic-vibrator and acoustic-spectrum-analyzer hardware obtained from the West had substantially improved Soviet sonar capabilities and their submarines' underwater stealth. The flow of Western technology, it was estimated, had allowed the Soviets to start research projects that had not been under consideration, to improve the technical sophistication of several thousand developmental programs per year, and to shorten the lead times for the manufacture of advanced hardware.

Given the international dimension of the problem, the Reagan administration moved strongly on the diplomatic front to revitalize American leadership. As early as 1981, his first year in office, President Reagan raised the issue of Soviet acquisition of Western technology at the Ottawa Summit. The next year, energized by U.S. concerns, senior officials of Western governments assembled for the first time since 1957 to discuss technology transfer issues. At approximately the same time, NATO and COCOM began to review the connection between trade and allied security.

Meanwhile, the Reagan administration pushed for greater international cooperation on prevention and enforcement

efforts. Late in 1983, for instance, the United States together with South Africa, West Germany, and Sweden foiled a covert Soviet operation to obtain critical parts of the American-produced VAX computer, used for missile guidance systems. The same year, NATO states expelled almost four times as many Soviet government officials for industrial espionage as in the previous year.

In addition to challenging clandestine Soviet efforts, the Defense Department and U.S. Customs Service established Project Exodus, directed against Western firms that tried to dodge rules governing the export of sensitive equipment. In its first three years, the effort seized 2,851 illegal shipments of defense-related equipment worth $177 million.[13] Project Exodus aimed not only at prosecuting smugglers—a small fraction of all exporters—but also at developing new methods to track illicit high-technology flows and increasing the training of customs agents.

Senior Pentagon officials began to bring up technology security issues at all meetings with foreign officials. One such meeting between Secretary of Defense Caspar Weinberger and his Japanese counterpart resulted in the public exposure in 1987 of Toshiba's role in supplying the Soviets with complex machine-tooling equipment. Combined with software from Norway, the equipment allowed the Soviet navy to improve its submarine propellers by reducing their noise and making the subs more difficult for NATO to detect. The Toshiba case was recognized as a serious breach of technology security and illustrated the complex international dimensions of the problem.

Meanwhile, to provide stronger policy control over technology exports, the Pentagon established a new office, the Defense Technology Security Administration (DTSA). With a director who carried the rank of Deputy Undersecretary of Defense, DTSA was to be "the focal point" of Defense Department efforts to keep international transfers of

defense-related technology "consistent with U.S. foreign policy and national security objectives."[14] Related government bodies, including the Defense Intelligence Agency, were directed to support the DTSA. This order was an important formal provision that gave the agency the bureaucratic clout it needed to receive timely information and act on it. In addition, a high-level official, the Assistant Secretary of Defense for International Security Policy, would provide senior representation for the Pentagon on technology-security issues in the interagency process, an important but often gridlocked system of consultations among executive branch departments.

The DTSA hoped to restrict the Soviet armed forces' ability to make significant technological advances by denying them the sophisticated microprocessors, high-powered computers, and other electronic equipment that served as "force-multipliers" for their military. The new organization's ban on the export of microprocessors, for instance, kept a key component of the then-new "look-down/shoot-down" radars (which provide aircraft with targeting information) out of Moscow's hands for nearly a decade. Later, using less powerful but now commercially available computer chips, Soviet radar still suffered a performance disadvantage.

In other areas, DTSA worked to prevent the export of sophisticated hardware that would have allowed the Warsaw Pact to jam NATO's high-frequency microwave communications. The agency also preserved restrictions on the export of "hot-section" metallurgy technology, an advanced manufacturing technology that produced aircraft engines with a 10,000-hour service life and thereby provided America an extraordinary edge over Soviet aircraft engines that operate only an estimated 200 hours before breakdown.

During the 1980s, the work of the DTSA contributed to a growing lead for American technology. According to its first director, Stephen Bryen, the gap between U.S. and Soviet

technologies was estimated by the CIA to have increased more than seven years during the decade, from about three years to more than ten. But the Soviets and the Warsaw Pact states were not the only potential adversary being denied U.S. technology. The DTSA also played a significant role in denying sensitive military technologies to potentially dangerous states in the Middle East and elsewhere. In the late 1980s, for example, the DTSA learned that Iraq was attempting to purchase 1.5 million self-injecting kits of an antidote to sarin, a deadly chemical nerve agent. Since no other state in the region possessed sarin, the DTSA argued, the antidote kits could only be intended by the Iraqis to protect their own military personnel during the conduct of chemical warfare. Over State Department objections, the sale was blocked.[15]

4
Relaxing Our Guard

Following the cold war, America's political leadership moved to change our export-control regimen. The Soviets had left the international scene. The arms race, at least the one that had grown familiar over the previous five decades, appeared defunct. Washington and Moscow agreed on a series of actions that would change the size, targeting, and immediate-alert status of their nuclear-tipped missiles. With the exception of Russia's nuclear capabilities—substantially discounted because of the new regime's apparent benignity—the horizon cleared of a peer-competitor who could seriously challenge the existence of the United States.

Accentuating the positive in the international security climate, the Clinton administration reduced the influence and scope of our export-control apparatus. The DTSA was downgraded to become a division under a new Defense Threat Reduction Agency (DTRA), whose primary missions were nuclear deterrence, reducing the nuclear threat, and countering the threat from chemical and biological weapons. The new agency reports to the Undersecretary of Defense for Acquisitions, a reporting arrangement that makes this official responsible both for downsizing defense contractors and for preventing those firms from compensating for the effect of this discipline through foreign sales.

The number of personnel assigned to DTSA was reduced by almost a fifth, from 145 to less than 120; it is likely to drop further as departing personnel are not replaced. In addition, associated Defense Intelligence Agency functions were drawn down: where fifty DIA analysts once monitored Soviet activities alone, today three keep track of the entire world.[16] These shifts sent a clear signal within the Pentagon bureaucracy that technology transfer had lost some of its priority. As a result, the military services and the Office of the Joint Chiefs of Staff, for example, began supplying information to DTSA "as time became available."

International controls on technology transfer were similarly eased. With the end of the Warsaw Pact threat, COCOM disintegrated. It was succeeded by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar"), named for the suburb of The Hague where the new accord was reached in 1996. Signed by thirty-three nations, Wassenaar was intended to be "the first global multi-lateral arrangement covering both conventional weapons and sensitive dual-use goods and technologies."[17] An international bureaucracy in Vienna receives and distributes reports from participants. The means of enforcement, however, are not robust: participating nations are to enforce their own export-control policies. In contrast to COCOM, there are no agreements among members that effectively prohibit specific exports, nor is there advance review of license applications.

One additional control is the Missile Technology Control Regime (MTCR), a voluntary, informal arrangement begun in 1987 and now signed by thirty-two nations. It concerns itself with the export of delivery systems and related technology for missiles capable of carrying a relatively large, 500-kilogram payload at least 300 kilometers, that is, beyond tactical range. U.S. law provides for sanctions against countries that violate MTCR guidelines, including

restrictions on the end-use of technology, but the regime's common export policies and its list of export items do not legally bind signatories.[18]

Taken together, these shifts in Washington and in international forums brought a reduction of export-control activity in the United States. The Defense Department is responsible for appeals to export permissions granted by the Commerce Department. During the Reagan and Bush administrations, this check on the process was regularly employed; during the Clinton years very few appeals were made.[19] In the mid-1980s, U.S. firms applied for licenses for the export of dual-use equipment at the rate of 150,000 per year. With fewer and fewer types of technology restricted by the end of the 1990s, applications dropped to approximately 11,000 per year.

The Department of Commerce is the principal federal agency responsible for controlling exports. Its Bureau of Export Administration (BXA) issues the licenses that American manufacturers require in order to export dual-use equipment. Licenses to export are granted depending upon an item's technical characteristics, the destination, the end-use, the end-user, and, as the Commerce Department puts it, "the other activities of the end-users," that is, the likelihood of proliferation.

To begin the process, a manufacturer must ascertain whether an item is classified as dual-use. The bureau issues a list covering nine categories, including nuclear facilities, sensors and lasers, navigation and avionics, and propulsion systems (including space vehicles). License processing currently averages more than a month's time, but varies by country: processing applications for exports to China takes more than two months.[20]

Exporting specific military and defense-related products may also require permission from other departments. Thus, the State Department's Office of Defense Trade Controls

rules on requests to export such items as automatic weapons, rifles with more than a .50 caliber bore, the components of these weapons, and ammunition. At Defense, the Defense Threat Reduction Agency considers requests to export larger defense-related equipment and machine tools. In addition, an informal consultative process exists among departments with qualified experts. The Pentagon provides approximately 21,000 recommendations each year on Commerce export license applications; the State Department, nearly 50,000.

The export-control system is widely perceived to be hampering legitimate commercial enterprise because of its complexity and lack of focus. Yet as complicated as the system can be, in practice, rejections and penalties appear to be few. In 2000, according to BXA, overall license denials appeared to be running at about 4 percent, down from 9 percent in 1999, when sanctions against India led to a spike in denials, and slightly more than the recent average of 2 to 3 percent. In the case of China, BXA reports approving 413 applications valued at $1.2 billion in the first six months of 2000; 21 applications, or only about 5 percent, were denied.[21] Penalties for trying to export equipment without a license can be low. Five years after the Republic-Lagun Machine Tool company of Carson, California, exported to China a vertical milling machine with its computer numerical controller (brain), capable of making sophisticated struts and internal engine parts for high-performance jet aircraft, the Commerce Department fined the company $20,000.

5
Slipping Through the System

In fact, despite the end of the cold war, dangers from technology transfer remain. Over the 1990s, as Soviet weaponry (along with the scientists who created it) poured out of a cash-strapped Russia onto international markets, concern about weapons proliferation grew. U.S. Secretaries of Defense from both political parties warned publicly about the potential spread of weapons of mass destruction and the means to deliver them over long distances, and the threat that this must eventually pose to America.

Moreover, this trend was occurring just as "dual-use" technology became as commonplace as buttons. Cell phones, pagers, weather satellites, global positioning satellite receivers, and the Internet—all elements of economic development around the world—have also brought sophisticated navigational, communications, and encryption capabilities within reach of countries like Iraq and North Korea, states where serious efforts had been underway for decades to possess complex and dangerous weapons.

The most active importer of American goods that require export licenses is China, with some 67 percent of all BXA controlled-list license applications in 1998.[22] The preponderance of dual-use high technology that finds its way to

China may be intended for legitimate civilian purposes, but by its own account, Beijing's military has a direct interest. A 1994 article by General Ding Henggao, then-chairman of China's effort to collect high-tech and military items, the so-called Commission on Science, Technology, and National Defense Industry, was explicit: "We must study defense-commercial dual purpose technology and possible transfers from commercial technology to defense use. Development of defense products should actively use commercial technology, so that it will have a solid foundation."[23] Lest there be any doubt about the propriety of acquiring Western technology, General Ding quotes Deng Xiaoping: "Science and technology are the common treasures of mankind. Every nation, every country should learn from the strong points of other countries, and learn from advanced science and technology of others."[24]

The Chinese military's interest in acquiring Western technology coincided with the liberalization of international transfer restrictions, as well as the growing participation of China in world markets. (China now accounts for some 3 percent of world trade, a share expected to grow with its participation in the World Trade Organization; its economy is estimated to be larger than that of Japan.[25]) Not surprisingly, technology with military applications began flowing out of the West to China.

Japan, for example, is a large exporter of dual-use equipment to China. Specific items include manufacturing technology needed to craft composites used in a wide variety of applications, including the making of stealth weapons. These transfers have been significantly facilitated through the use of foreign subsidiaries based in Hong Kong and Singapore. German companies have also sold important production technologies like high-temperature furnaces to China, improving the People's Liberation Army's ability to make the composite materials used in such military

applications as the nose cones and nozzles of intercontinental ballistic missiles.

One critical area involves machine tools, desirable because they give an importing nation the capability to build its own equipment rather than having to depend on others. Unlike yesterday's drill presses, crank-pin grinders, or turret lathes, today's "multiple-axis" tools can mill the very complex shapes required for the manufacture of, for instance, submarine propellers silent enough to avoid acoustic detection as they drive 16,000 tons of metal through the water, or jet-engine components whose extraordinary tolerances give aircraft great speed and maneuverability.

While China can produce less-sophisticated machine tools, it did not as of the end of 1996 possess the ability to mass produce five- or six-axis machine tools to Western standards—standards capable of supporting the production of advanced weaponry. In 1993, McDonnell Douglas Corporation sought licenses to export nineteen such machine tools to the China National Aero-Technology Import and Export Corporation (CATIC), a principal purchasing arm of the People's Liberation Army. The tools, said CATIC, would be used to manufacture commercial aircraft, as specified in a 1992 agreement with McDonnell Douglas known as the Trunkliner program.[26] CATIC subsequently modified its contract, halving the number of commercial aircraft to be built from forty to twenty, and shifting the factories for which the tools were designated. The U.S. administration allowed the export of nineteen machines in fall 1994. Within a year, the Commerce Department learned that, in violation of the export licenses, six of the American machine tools had been sent to an unapproved factory in Nanchang, eight hundred miles south of Beijing, whose output included military aircraft and cruise missile components.[27] The case remains under investigation.[28]

High-tech machine tools are the indispensable condition for precision manufacturing, but an aspiring imitator with the right machine tools also requires something to copy. In 1992, the Defense Department learned that negotiations were underway between PRC officials and Allied Signal's Garrett Engine Division to coproduce jet engines, which had been removed from the restricted export list the year before. After an interagency review, the coproduction deal was blocked, but the sale of engines was allowed to proceed. The Defense Department has concluded that China is now well on the way to possessing the ability to manufacture world-class high-performance jet engines.[29]

Numerous other technology sales have been facilitated by dispensing with or liberalizing defense export controls.[30] These include low-observable (stealth) technology, telecommunications, high-powered computers, encryption, and missile and satellite technology. Some key cases include:

- Communications satellites such as the Asiasat; Chinastar; Chinasat; and APSTAR 1, 2, and 2R, manufactured in large measure by Hughes and Loral. Beginning in 1993, the Clinton administration waived restrictions that had prevented the export of these satellites and recategorized them as dual-use equipment, not munitions, which allowed them to avoid Defense Department review. The sale of the satellites, which are deployed in clusters from the nose cone of a single rocket, raised concerns that China would acquire valuable insight into a related problem of orbital technology: how to launch several warheads from one nose cone. The satellites could also augment Beijing's police surveillance and intelligence capability by enabling the regime to monitor communications inside and outside China's borders. Following adverse publicity, Congress put these telecommunications satellites back on the

restricted munitions list in 1999; China, however, had already acquired and placed in orbit two satellites.[31]

- Computer switching equipment, which the Clinton administration allowed to be sold to China without Defense Department review. Asynchronous Transfer Mode and Synchronous Digital Hierarchy switching equipment can route voice and electronic messages around a country's communications systems, including through lines buried in the ground. By making signals difficult to intercept and protecting lines against physical attack, the equipment can materially strengthen the possessor's command and control network.
- High-temperature furnaces, approved for sale to China in 1998. This technology does have a civilian use, albeit one with a seemingly limited market: making titanium prostheses such as artificial legs and arms. Perhaps more significantly, high-temperature furnaces are required to craft the very pure metals and composite materials needed to manufacture missiles, nuclear weapons, and stealth aircraft.

In all, the satellites, switching equipment, fiber optics, and other technologies that our liberalized export controls placed in China's hands have helped that country build an advanced command, control, communications, computers, and intelligence network whose sophistication has significantly improved China's military prowess.

6
Sold and Sold Again

Military-related exports to China also have a global impact through China's own exports, which are a principal conduit of restricted Western technology to rogue states and proliferators. China's foreign military sales took a quantum jump beginning in about 1996. They have included high-quality specialty steels required to produce missiles, sent to Iran, North Korea, Pakistan, and Syria; solid missile propellants, sold to Egypt, Iran, Libya, and Pakistan; missile-guidance accelerometers and gyroscopes, sold to Egypt, Iran, Libya, and Pakistan in 1997; and parts for Pakistan's nuclear program and assistance in building its M-11 ballistic missile.

As of this writing, Iran, a major beneficiary of China's exports, has a near-operational Shahab-3 medium-range ballistic missile, with a range of some eight hundred miles—able to reach, for example, Turkey, India, or Israel from Iran's soil. The Shahab-5 may be ready by 2003; its estimated range is as much as 3,600 miles—enough to reach all of Europe and most of Asia. China is known to have helped with Iran's chemical weapons capability, as well as its Nuclear Buskia Zero Power Nuclear Reactor and Graphite facility, from which weaponized nuclear fissile material can be obtained.

In few of these destabilizing and proliferating sales did the United States take strong action. In 1994, China sold

Pakistan parts of a missile with a payload of at least 1,100 pounds and minimum range of 185 miles, in violation of the Missile Technology Control Regime, an accord that Beijing promised to honor. The Clinton administration offered to forgive China if it would admit its violation; Beijing admitted nothing. When the PRC sold Iran C801/802 Silkworm antiship missiles—which could endanger U.S. Navy operations in the Persian Gulf—the Clinton State Department simply issued a démarche (a mild diplomatic protest called a "demarshmallow" in diplomatic circles), even though American machine tools and specialty furnaces sold to China had contributed to improving the capabilities of the Silkworm missiles that China sold Iran.

The United States was also slow to act when specialty steels that could only be used to make SCUD missiles went from China to North Korea and Syria. Titanium-stabilized duplex stainless steel has virtually no commercial applications; it can be, and is, used in the production of SCUD missiles and in the storage of their highly caustic propellants. Despite evidence that a third country was selling this highly specialized steel to China, it took the Clinton administration two years to place it on the list of materials whose export is proscribed by the Missile Technology Control Regime. In this as in the other issues raised by China's stealthy effort to increase its military's technological sophistication, the Clinton administration steadfastly refused to apply sanctions, to use its leverage to withhold other goods Beijing wanted, or to discourage China's problematic behavior in any meaningful way.

With the outpouring of formerly restricted technology to China—and by extension, to its rogue-state clientele—development times for military hardware have been dramatically compressed. In December 1999, the *Washington Times* carried reports that a Chinese submarine, the Type 094, would be operational around 2005. The sub will carry the

Julang-2 ("Great Wave") missile, an intercontinental ballistic missile capable of reaching a target 7,400 miles away, which will permit Chinese submarines to threaten cities throughout the United States.[32] Pentagon officials said that the Julang-2 would be armed with Chinese copies of the small-size, large-power W-88 warhead—whose design had been stolen from the United States, as Bill Richardson, the Clinton administration's Secretary of Energy, admitted in March 1999.

China's enhanced ability to project nuclear force is noteworthy not merely for its threat to America but also because much of the Clinton administration's decontrol of defense exports took place after 1995, when the administration first admitted that China may have stolen our W-88 warhead design. For example, the export to China of computers that could be used to test the performance of nuclear warheads continued even *after* the administration knew what had likely happened to the W-88 design. Similarly, the machine tools for the quiet submarine propellers were delivered in China *after* the administration realized the extent of Beijing's success in appropriating our advanced nuclear weapons technology.

7
Toward a New Policy

A policy as unconcerned about exports of critical defense hardware as the Clinton administration's was is not in the nation's interest. More careful attention must be paid to securing the priceless asset of America's technology.

At the same time, if we are to design a more effective system of technology security, we must first understand its goals. The free-trade policies central to American international leadership since the end of World War II have played a critical role in our prosperity and the world's. Under these circumstances, only the clearest proof of threat and the knowledge that a response will be effective can justify export controls.

Even in the mid-1980s, with a threat as obvious and dangerous as the Soviet Union, the revitalization of COCOM was politically difficult, both at home and abroad. Today's global web of commercial relationships has led some observers to focus almost exclusively on the difficulty of controlling dual-use technologies. In a 1998 interview, then-Secretary of Defense Bill Perry compared the effort to control information technology to "trying to sweep up the sand on a beach."[33] Laura D'Andrea Tyson, President Clinton's chief economic adviser in 1996, wrote that trying to prevent the export of dual-use technologies is futile: "The U.S. is not

the only source for such products, so a unilateral ban only serves to drive global customers to competitors."[34]

Admittedly, the openness of today's world economy and the expanding zone of private enterprise have promoted the spread of information, for good or ill. While the United States must make serious efforts, where possible, to stop the export of critical defense technologies, we cannot trust in these measures alone as guarantors of our security.

America's strategic strength, the heart of our armed power, is the technological edge that enables us to field the world's most powerful military. Our fundamental aim must be to ensure that our technology remains the best—and that we effectively turn this technological leadership into real military advantage by crafting strategies that force potential enemies to vie with us militarily in the areas of our greatest technological and creative strengths. This principle suggests certain guidelines for more effective defense export controls in the twenty-first century:

- First, for products that are critical to a potential opponent's military capability, and whose transfer we can control, the cold war method of export restrictions continues to be sensible. The intersection of military use and controllable transfer is a choke point we can exploit. We need not stand by as others attempt to turn our own technologies against us.
- Second, for products that are critical to a potential opponent's military capability, but are either widely available or becoming so, export restrictions are less effective than a strategy of maintaining a clear and undeniable American technological lead.

8
Finding America's Strategic Center

To understand the evolving center of our forces' superiority—and thus to shed light on how to protect critical products of American manufacture—the American Enterprise Institute assembled a panel of three distinguished defense experts. We asked Professor Alvin H. Bernstein of the National Defense University; Mr. Laurent Murawiec, a senior analyst with RAND; and Mr. Tom Donnelly, deputy director of the Washington-based Project for the New American Century, to consider this question: What will the strategic center of America's military superiority be over the next three decades?

Their answers paint a picture of warfare dramatically transformed by the spread of technology. To maintain and increase its military dominance, the panel agreed, the United States must take full advantage of the asymmetry that gives us a head start in space, cyberspace, bioengineering, and various forms of technology-dependent warfare that sophisticated states are best able to develop and deploy. Our objective must be to maintain and increase our lead in these areas.[35]

The panel agreed that many key innovations with military applications, such as cellular communications, global positioning satellite receivers, and direct broadcast satellite

receivers, can now be purchased the world over. They warned that the spread of these technologies, and the openness of the West's engineering graduate schools to foreign students, can put America's ability to maintain military forces in distant theaters at risk. The United States could within the foreseeable future be forced to shift its focus from how to exploit superior U.S. technology against an enemy, to how to prevent that technology from being used against us.

The panelists emphasized several areas of strategic importance in maintaining the United States' military advantage. First is the development of a mature ability to exploit warfare in space. Space and cyberspace, Mr. Murawiec noted, are the twenty-first-century equivalent of the nineteenth-century battlefield's "high ground." The U.S. military's control and exploitation of that ground—through the deployment of space weapons systems, intelligence-collection mechanisms, and tools to manage the earthly battlefield—are key to victory over an enemy. Among other steps, Professor Bernstein recommended a research and development strategy that concentrates on the improvement of electronic sensor technology.

The panel noted other strategically critical areas:

- Nanotechnologies: microscopic and chemical devices that operate at the molecular level to produce extraordinary advances in computing speed, software, and the surge capacity of our manufacturing capability, which has been a foundation of American victory since the Civil War;
- Energy for photovoltaics, compact storage, and beam delivery;
- Software advances;
- Manufacturing technologies that will allow the efficient mass production of all these components; and

- Lift: the ability to move powerful forces swiftly around the world. Panelists noted the need for lightweight fuels, compact power units, and lighter, more precise ordnance that will reduce the cost and burden of transportation.

These ideas have straightforward policy implications: America's technology must continue to outperform that of potential rivals. For a nation supported by innovation and enterprise, a nation whose national security has depended importantly on productive capability, the key to future security will be to do what we do best: invent, adapt, and advance. We must guarantee that the edge of our leading technologies stays sufficiently ahead of any potential opponent that it will deter or—if necessary—defeat him.

9
The Case of the Computer

The challenge of designing an export-control regime for today's world lies in the fact that many technologies critical to military capability are products not of military research but of the commercial marketplace. These same technologies are dynamically changing and also widely available on a global scale. Computing power is a good example.

In December 1992, the Bush administration considered a request by the Cray Research Company of Minneapolis to export supercomputers to China. Such computers—capable of performing 950 Millions of Theoretical Operations Per Second (MTOPS)—had been restricted under provisions that capped the performance of exportable computers at 13 MTOPS. The rationale for those caps was the fact that more powerful machines had valuable military functions; the Cray computers, for instance, were capable of modeling the effect of nuclear blasts on the atmosphere. State Department advocates of this proposed sale argued that the computers would serve humanitarian purposes by improving China's ability to forecast monsoons.[36] Although President Bush rejected this argument, no decision was reached before the Clinton administration took office in January.

The incoming Clinton administration ultimately approved the sale and gradually lifted the upper limits of computing ability, as measured in MTOPS, that American manufacturers

are permitted to sell abroad. In 1993, the ceiling rose to 195 MTOPS; in February 1994, it was revised upwards to 1,500 MTOPS; in 1996, after a Stanford University study concluded that computers rated at 4,000 to 5,000 MTOPS (and soon 7,000 MTOPS) were already available the world over, the export cap was raised to 2,000 MTOPS. At the same time, the administration divided importing countries into four tiers, with varying levels of restrictions. Tier-3 countries (including Russia, China, India, and Israel) could import computers rated up to 7,000 MTOPS without a license, provided that the end-user had a legitimate civilian purpose. Exports for military use could not exceed 2,000 MTOPS without a license.

In the following year, political debate increased over the Clinton administration's China policy, including its export controls on computers. Congress attached a provision to the 1998 fiscal year budget which forbade sales of American computers with 2,000 MTOPS or more to tier-3 countries without the U.S. government's advance approval. The legislation passed despite strong concerns from the computer industry, which knew that microprocessor power was accelerating at macropower speeds.

In fact, the U.S. government's retreating MTOPS goalposts were trailing Moore's Law, a theorem named for the engineer Gordon Moore, chairman emeritus of Intel Corporation, who theorized that the power of microprocessors (chips) was doubling approximately every twelve to eighteen months. The exact numbers and subsequent revisions of Moore's Law are less important than his basic insight: computing power is advancing at a speed of innovation unknown in history. Indeed, today's off-the-shelf, single microprocessor laptop computer possesses more than two-and-a-half times the power, and sells for about 1/2,500th the price, of the Cray machine upon whose sale to China the Bush administration could not agree.

A transistor is the electronic component originally designed to amplify a radio's signal. In computers, it is the microscopic switch that performs at extremely high speed the millions of yes-or-no decisions upon which computer programs depend. In the quarter-century from 1971 to 1998, the number of transistors contained in a single computer chip increased more than 3,200 times, from 2,300 to 7.5 million. In turn, the numbers of operations per second that computers could perform skyrocketed.

By mid-1999, the unreasonableness of the 2,000 MTOPS limitation could no longer be ignored. The administration raised the level of what could be exported to tier-3 countries to 6,500 MTOPS; limits for machines sold to a civilian end-user moved up to 12,300 MTOPS. Early in February 2000, the Clinton administration announced another increase in the tier-3 MTOPS export cap, which was raised to 12,300 for military use computers, 20,000 for civilian use. In August 2000, the administration announced its intention to move the tier-3 cap to 28,000 MTOPS and eliminate the distinction between military and civilian end-use.[37]

Meanwhile, throughout the world, computing power continues to skyrocket. When Intel's "Itanium" chip appears on the market, it will be rated at 5,600 MTOPS. Since most business machines use three or four processors, the imminent increase in computing power will lift the power of easily available machines to nearly 25,000 MTOPS. That is enough, according to a 1998 Stanford study, to design military aircraft and develop nonacoustic antisubmarine warfare sensors. It is enough to drive some synthetic-aperture radar applications designed to see through inclement weather and to model turbulence around aircraft under the stress of combat flight conditions. It is enough to design and develop advanced combat aircraft, to model the impact of blasts on underground and surface structures, and to

forecast difficult meteorological events, such as the effects of atmospheric nuclear blasts.[38]

Nonetheless, computers with 25,000 MTOPS are also useful to businesses with a high volume of message traffic and heavy demand for Internet services. As a result, the Itanium chip and its eventual peers are likely to become the chips of choice in the radically compressed future that galloping microprocessor technologies have called into being. If the United States is going to try to control the export of computers based on these chips, it might as well try to regulate the outflow of spoons.[39]

In the late 1990s, the public revelation of Chinese efforts to steal American nuclear secrets threw fuel on the heated debate over exports to China, including computer sales. In 1998, the House of Representatives established a bipartisan Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, called the Cox Committee after its chairman, Representative Christopher Cox (R-Calif.). Recognizing both the importance of computers as well as their distinction from other defense-related technologies, the committee devoted an entire chapter of its final report to the sale of American high-powered computers to China. Ultimately, however, the report failed to distinguish between what can and cannot be effectively controlled through export restrictions.

Effective export controls limit the sale abroad of hardware (1) without which a potential adversary cannot achieve specific military objectives, (2) over which the manufacturing nation has effective control, and (3) for which there are no substitutes. Computers fail two of these fundamental tests. Although they are indeed critical to a modern military for everything from logistics to weapons-design to fire-control radar, their widespread commercial availability makes it virtually impossible to prevent their being

exported. Anyone can walk into a computer store, buy powerful machines, and take them abroad to build or strengthen already existing networks of computers.

Indeed, with the exception of extremely powerful, nearly unique machines such as IBM's Big Blue (with its 1.6 million MTOPS) or the projected 2.5 *billion* MTOPS computer for genetic research, computers are easily obtainable, and they are produced in large numbers abroad, for example in Japan and Taiwan. These realities make control of all but the rarest machines an exercise in futility.

This situation differs sharply from that of technology with a primarily military purpose, such as machine tools designed to fashion complex surfaces for uniquely military specifications, sophisticated metals and metallurgical processes needed to manufacture missiles, satellite technology useful for advancing intelligence gathering, command and control systems, and critical components of high-performance jet engines. These and similar defense technologies are costly, few in number, and focused on military purposes. Where the United States holds an effective monopoly on the technology, its spread is controllable; where the United States does not have a monopoly, we can exercise effective leadership in international forums.

10
A New Balance

As memory of the cold war fades, people will find the end of the U.S.-Soviet antagonism less and less important. The constants of international power—competition, conflict, and the long marches of nations to and from global prominence—will reoccupy the world's attention.

To pursue its own interests while remaining true to itself, the United States must not retreat from its international leadership position as the principal supporter of free markets and free trade. The porous borders, transparency, and freedom of movement that characterize American policy promote a safer, more prosperous world.

Staying the free market and free trade course need not conflict with U.S. efforts to keep technology of its own making from falling into dangerous hands. Those hands are not still; they are working as hard as ever. The important difference is that our guard is down, international economic competition is up, technological change is galloping forward, and the sources of potential danger to national security are many—including China, with its deliberate policy of proliferation and increasing wealth.

American policy should reflect these facts. The nation's technological advances help propel both our productivity and the world's economy. But these advances also offer an important edge to America's defense upon which our

economic security ultimately rests. The United States must protect both as it seeks a new balance between the linked goals of economic and technological security.

Like any public policy, an export-control regimen must aim at something. The Clinton administration's policy aimed at nothing. Because no idea of the nation's critical strategic strengths informed our policy, we lacked any notion of what to protect, much less how to protect it. The Clinton administration's policy was consistent only in its lenient decisions about the export of genuinely sensitive and controllable defense technologies.

To begin repairs in the new administration, policymakers must first clarify the export-decision matrix. In an era of exploding commercial high technology, where children's games now carry more computational power than was once used to launch space probes, it is time to reconsider the usefulness of the "dual-use" designation. Virtually all basic technology of concern is now dual use. A better focus for national security would be to ask, first, whether a technology has significant military uses; second, whether it is controllable by the United States.

In the matrix below, one axis represents the potential uses of defense-related technology, ranging from critical military technologies with virtually no legitimate civilian use, to commercial technologies with significant military applications. The second axis represents the degree of U.S. control over the transmission of the technology, ranging from an environment that is primarily U.S. controlled, to an open, vigorous world market of competing suppliers.

Clearly, these categories are porous, and products can shift position due both to market and technological change. But if we use the matrix as an analytical framework, the United States' export-control decisions fall into four broad categories.

Decision Matrix for Controlling Dangerous Technologies

	Primarily a U.S. Technology	*World Market in Technology*
Critical Military Technology; virtually no civilian use	control exports + maintain U.S. tech edge	build U.S. tech edge + lead nonprolif. effort
Commercial Technology with Significant Military Application	monitor, license, restrict tech transfers + develop U.S. tech edge	lead int'l tech transfer restrictions + build U.S. tech edge

Militarily critical technologies, with virtually no legitimate civilian use. These are the clearest subjects for strict export controls. At the same time, America should strongly invest in maintaining its military lead in these technologies. In today's rapidly changing world, leadership in advanced technologies cannot be taken for granted.

Critical military technologies in which a world market already exists. Here, with proliferation already a fact, it is imperative to restore or maintain a failsafe U.S. technology edge. In the case of weapons of mass destruction and other dangerous armaments, the United States should also be leading a vigorous international effort to restrict their further spread, using a full range of diplomatic, economic, military, and other instruments.

Advanced commercial technologies with significant military applications, whose market is controlled or dominated by the United States. Here, the commercial role of the technology must be respected as well as balanced against its potential military dangers. An effective regimen will take a sophisticated approach to controlling exports through monitoring, licensing, and restricting the

technology, taking into consideration both the end-user and end-uses. At the same time, because commercial markets spread technology, and because rapid changes in commercial technologies drive military advances, continuing defense research and development in these areas should be a priority.

Commercial technologies with significant military applications that are already widely available on the world market. Efforts to control these unilaterally are doomed to failure. Worse, such controls impede the development of the U.S. market in the technology at issue, as well as the advances that result from the free market. For this reason, export controls over these products should primarily be part of an international technology-transfer regimen in which the United States takes a leadership role. Above all, the United States should be actively developing these military-related technologies in order to sustain its lead over potential adversaries. We must also act wisely to protect against the technological vulnerabilities that the spread of knowledge has caused.

11
Recommendations

Within this framework, this study on defense export controls after the cold war makes the following recommendations.

First, the Defense Department should immediately assess technologies critical to America's future military advantage and determine which advanced technologies are least accessible to potential competitors. This assessment should include what potential adversaries may have acquired from the United States and other international sources since the end of the cold war, as well as the possible effects on our national defense.

Second, authority and effectiveness must be restored to the export-control system by making sharp distinctions between controllable and uncontrollable technologies. National security is not advanced by placing unilateral U.S. export controls on commercial technologies that are widely available from many suppliers and actively traded on world markets. In the information industry, for instance, the government's use of MTOPS as an export standard and its focus on general-purpose computers built for commercial purposes have set technology controls on a losing race against the development of more powerful computers. Instead, government should concentrate on preventing the export of those few extremely powerful, high-end machines that provide a significant military advantage. To develop such a

standard, the Pentagon should establish a working group that includes technologists, scientists, defense experts, and representatives of the computer and microprocessor manufacturers.

Third, because effective American control of dual-use technology requires strong, effective international cooperation, the Wassenaar Arrangement must be strengthened. The United States should take the lead in renegotiating Wassenaar to provide (1) a specific list of importing countries of concern, including China; (2) a highly focused list of critical technologies of military significance; (3) a more effective process for prior review before sensitive exports are licensed; and (4) mandatory national sanctions against violators. Unless this is done, Wassenaar is worse than useless because it creates the illusion that we have effective export controls. Unless and until Wassenaar can be made to work, the United States should pursue an interim arrangement among a smaller group of countries that are serious about technology security.

Fourth, the Defense Department should replace the Commerce Department as the leading cabinet-level department for issuing export licenses. During the cold war, wide understanding of the dangers of Soviet aggression assured respect for national security considerations, and thus having Commerce as the lead department ensured commercial interests were given sufficient weight. Today, the balance has reversed: commercial concerns are widely understood, national security issues less so. As the major organ of the U.S. government with the expertise to protect the nation against the dangers of advanced technologies, the Department of Defense should take the lead in export controls, with the Commerce Department fully empowered in the interagency review process.

Fifth, Congress and the administration should simultaneously upgrade the Defense Department office responsible for

technology-transfer policy and its application. The Defense Technology Security Administration's expertise and independence of action are needed to provide the strong leadership this critical issue requires. To reduce the negative impact on U.S. business, the process of issuing export licenses must be speeded up. American manufacturers have a legitimate complaint that the current process takes too much time and results in a competitive disadvantage for U.S. companies.

Sixth, given the reality of spreading technologies, the United States should increase its investments in maintaining and extending our technological edge. Military strategy should force potential enemies to vie with us militarily in the areas of technological creativity where they cannot hope to best us. Nanotechnologies and the unique surge capacity of American industry are among the creative strengths that dishearten potential enemies. In the key area of information technologies, as the panel of defense experts noted, we need to advance military-related technologies and the pace of innovation to outstrip a rapidly developing field. Practical steps could include support for promising graduate students in key sciences; joint ventures among government, academia, and business; and focused tax incentives that reward investment in research. Such policies will provide far more tangible gains in national security than ineffective export controls.

Seventh, along with efforts to increase the United States' technological edge, we must also concentrate on defending our existing technologies—from nuclear secrets, to applied biological and genetic research, to the computer infrastructure critical to the nation's economy. In January 2000, the Clinton administration announced a plan to focus attention on the vulnerability of U.S. commercial computer networks. In the months that followed, cybervandals forced the closing of major web sites and used epidemic virus attacks to

shut down e-mail systems (including, CNN reported, those of the Defense Department and the CIA). Terrorists and rogue states are likely also to be aware of our potential vulnerability. Acting to prevent such attacks is essential.

Alexis de Tocqueville noted that there must "be a close link and necessary relationship between…freedom and industry." Freedom to benefit from one's inventiveness and imagination is a powerful force for prosperity. The same practical creativity built an American military that has stood fast in defense of our freedom. It is time for the United States to restore its stewardship of the critical technologies that have made us both prosperous and safe.

Appendix

Sensitive Technology Activity, 1998

EXPORT LICENSE APPLICATIONS AND DOLLAR VALUES, 1998

Country	*License Applications*	*Percent*	*Value ($000s)*	*Percent*
Albania	1	c	15	c
Armenia	6	c	a	c
Azerbaijan	3	c	1,397	c
Belarus	7	c	54	c
Bulgaria[b]	31	1.7	5,611	0.2
Cambodia	3	c	433	c
China	**1210**	**66.9**	**1,365,916**	**37.1**
Cuba[b]	21	1.2	183,970	5
Estonia	31	1.7	1,859	c
Georgia	4	c	115	c
Kazakhstan[b,d]	45	2.5	1,532,700	41.6
Korea, PDR[b]	2	c	1	c
Kyrgyzstan	2	c	20,095	5.5
Laos	0	c	0	c
Latvia	27	1.5	2,238	c
Lithuania	21	1.2	2,201	c
Moldova	1	c	3	c
Mongolia	0	c	0	c
Romania	49	2.7	4,933	0.1
Russia[b]	245	13.6	39,446	1.1
Tajikistan	0	c	0	c
Turkmenistan	4	c	493,250	13.4
Ukraine[b]	48	2.7	3,559	c
Uzbekistan	6	c	7,318	0.2
Vietnam[b]	39	2.2	13,213	0.4
TOTAL	*1806*	*100*	*3,678,312*	*100*

Source: U.S. Department of Commerce, Bureau of Export Administration, 1999 Annual Report, Appendix I.

a— less than $1,000

b— not including items subject to the EAR N.E.S. & not on the Commerce Control List

c— less than .1%

d— includes spacecraft [totaling $1.522 billion]

Notes

1. Charles-Louis de Secondat, Baron de Montesquieu, *Considerations on the Causes of the Greatness of the Romans and Their Decline*, trans. David Lowenthal (Indianapolis: Hackett, 1999), 214.
2. International Monetary Fund, *World Economic Outlook 2000* (Washington, D.C., 2000), 52, based on calculations by Bradford J. Delong, "Estimating World GDP One Million BC-Present," http://www.j-bradford-delong.net/TCEH/1998_Draft/World_GDP/Estimating_World_GDP.html (accessed on May 10, 2001).
3. Alan Greenspan, "Structural Change in the New Economy," remarks before the National Governors' Association, Ninety-second Annual Meeting, State College, Pennsylvania, July 11, 2000, http://www.federalreserve.gov/boarddocs/speeches/2000/20000711.htm (accessed on May 10, 2001).
4. U.S. Department of Commerce, Bureau of Economic Analysis, Selected National Income and Product Accounts Tables 1.1, 1.2, and 7.1, http://www.bea.doc.gov/bea/dn1.htm (accessed on May 10, 2001).
5. Washington data from a Statement on International Trade by Governor Gary Locke, published by *Across Borders,* an Internet law journal at the Gonzaga University School of Law, http://law.gonzaga.edu/borders/documents/locke.html (accessed on June 22, 2001). Oregon data from "Oregon's Exports from Its High-Technology Industry," a news article on the Portland State University School of Business Administration website (no longer accessible). Data on New Mexico are from New Mexico, Economic Development Department, http://www.edd.state.nm.us/TRADE/SUMMARY/indclass.htm (accessed on June 22, 2001). Pennsylvania data from Route 422 Business Advisor, http://www.422business.com/articles/199806/pahightech.html (accessed on June 22, 2001).

6. *Executive Summary of the Report of the Commission to Assess the Ballistic Missile Threat to the United States*, pursuant to Public Law 201, 104th Congress, July 15, 1998, 12.
7. "China is both a source and transfer agent for passing knowledge, technology, subsystems and entire systems to dangerous states and transnational actors." *Report of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction*, pursuant to Public Law 293, 104th Congress, July 14, 1999, 2–3. Also see the report of the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China (the "Cox Report"), May 1999, http://hillsource.house.gov/CoxReport/report/welcome2.html (accessed on May 16, 2001).
8. Most member states' lists of proscribed equipment were also closely held. See Linda Melvern, Nick Anning, David Hebditch, and Mark Hosenball, *Techno-Bandits* (Boston: Houghton-Mifflin, 1984), chap. 14.
9. Ibid., 264.
10. See William A. Root, "Trade Controls That Work," *Foreign Policy* (Fall 1984).
11. See Richard Staar, "The High-Tech Transfer Offensive of the Soviet Union," *Strategic Review* (Spring 1989).
12. U.S. Department of Defense, *Soviet Acquisition of Militarily Significant Western Technology: An Update* (Washington, D.C.: Government Printing Office, 1985).
13. Melvern et al., *Techno-Bandits*, quoting "High Tech Sting," *Time*, February 27, 1984, 75.
14. Caspar Weinberger, *The Technology Security Program, A Report to Congress*, 1986.
15. Author's interview with Stephen Bryen, November 9, 1999.
16. Author's interview with Mike Maloof of the Defense Threat Reduction Agency, November 10, 1999.
17. U.S. Department of Commerce, Bureau of Export Administration, "National Security Export Controls and the Wassenaar Arrangement," http://www.bxa.doc.gov/Wassenaar (accessed on June 15, 2001).
18. "The Missile Technology Control Regime," Arms Control Association backgrounder, August 2000.
19. Laura D'Andrea Tyson, "Washington Can't Keep High Tech to Itself, So Why Try?" *Business Week*, July 6, 1998, 18.
20. U.S. Department of Commerce, Bureau of Export Administration Update, July 10, 2000.

21. Ibid.
22. U.S. Department of Commerce, Bureau of Export Affairs, Fiscal Year 1999 Annual Report (Washington, D.C.: Government Printing Office, 2000). See Appendix, page 45, above.
23. Quoted in Michael Pillsbury, ed., *Chinese Views of Future Warfare* (Washington, D.C.: National Defense University Press, 1998), 160.
24. Quoted in ibid., 166.
25. Alan Greenspan, "Permanent Normal Trade Relations with China," remarks at the White House, Washington, D.C., May 18, 2000, http://www.federalreserve.gov/boarddocs/speeches/2000/20000518.htm (accessed on May 16, 2001).
26. This and the Garrett Engine case study are based on information from the Cox Report. See note 7, above.
27. Ibid., chap. 10.
28. Among other examples of machine-tool transfer, one Pentagon official told AEI that machine tools sold to China, including precision grinding machines manufactured by the Cincinnati Milicron company, had allowed Chinese arms manufacturers to improve the engines and capabilities of Silkworm cruise missiles.
29. See testimony of Dr. Stephen D. Bryen before the Senate Armed Services Committee, July 9, 1998.
30. Detailed information was assembled by Congressman Curt Weldon (R-Penn.).
31. Our intelligence services may benefit from these satellites by listening to the transmissions that move through these earth-orbiting phone banks. But China knows this too.
32. Bill Gertz, "U.S. Secrets Aboard Latest Chinese Sub," *Washington Times*, December 6, 1999.
33. "Preventive Defense and U.S. Diplomacy: An Interview with William Perry," *Stanford Journal of International Relations* 1, no.1 (summer/fall 1998), http://www.stanford.edu/group/sjir (accessed on June 25, 2001).
34. D'Andrea Tyson, "Washington Can't Keep High Tech to Itself," 18.
35. A transcript of panel presentations is available at http://www.aei.org/past%5Fevent/conf0120.htm.
36. R. Jeffrey Smith, "U.S. Postpones Decision on Supercomputer Sale," *Washington Post*, December 5, 1992.
37. U.S. Department of Commerce, Bureau of Export Administration, "High Performance Computer Export Controls," August 3, 2000 announcement.

38. Seymour Goodman, Peter Wolcott, and Patrick Homer, *High-performance Computing, National Security Applications, and Export Control Policy at the Close of the Twentieth Century*, http://iis.stanford.edu/lasso/iispubsrch.lasso?-database=pubs&-layout=detail&response=pview.lasso&-recordID=32896&-search (accessed on May 16, 2001).
39. A parallel debate exists over controls on the export of encryption software, which can ensure computer users (from businessmen to terrorists) of the security of their communications. Encryption has great commercial use: for example, it allows the secure sending of credit card information over the Internet. And Public Key Infrastructure (PKI)—the process that allows the transmission of scrambled information that can only be decoded by the two key holders, sender and receiver—is critical to the Internet's growing commerce. European states had commercialized PKI technology profitably. In the United States, Congress spearheaded change, responding to industry concerns that the prohibition on encryption exports would accomplish nothing except to put U.S. firms at a commercial disadvantage.

    Bowing to this pressure, the Clinton administration in 1998 allowed American software companies to sell 56-bit Data Encryption Standard software overseas. Defense, intelligence, and law-enforcement concerns prompted objections to liberalizing controls on this software. But the effort to control this technology became a dead letter once it was widely available. Moreover, as the number of calculations that a computer can make in one second becomes astronomical, so does a computer's ability to crack codes: In June 1998, the Electronic Frontier Foundation cracked a 56-bit encrypted message in less than three days using a specially designed computer that cost less than $250,000. See, among other sources, Ted Bridis, "Encryption Export Rules Relaxed," Associated Press, September 17, 1998.

About the Author

SETH CROPSEY is a director with the government affairs division of Greenberg Traurig in Washington, D.C. From 1999 to 2001 he was a Visiting Fellow at the American Enterprise Institute. He has taught at the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany. His government service has included serving as deputy undersecretary of the navy, assistant to the secretary of defense, and director of policy for the U.S. Information Agency's Voice of America. He is an officer in the U.S. Naval Reserve and is founder and chairman of the Adobe Foundation. His work has appeared in such journals as *Foreign Affairs, The National Interest, Commentary, Fortune,* and the *Wall Street Journal.*

The American Enterprise Institute for Public Policy Research

Founded in 1943, AEI is a nonpartisan, nonprofit research and educational organization based in Washington, D.C. The Institute sponsors research, conducts seminars and conferences, and publishes books and periodicals.

AEI's research is carried out under three major programs: Economic Policy Studies; Foreign Policy and Defense Studies; and Social and Political Studies. The resident scholars and fellows listed in these pages are part of a network that also includes ninety adjunct scholars at leading universities throughout the United States and in several foreign countries.

The views expressed in AEI publications are those of the authors and do not necessarily reflect the views of the staff, advisory panels, officers, or trustees.

Nelson W. Polsby
Heller Professor of Political Science
University of California, Berkeley

George L. Priest
John M. Olin Professor of Law and Economics
Yale Law School

Thomas Sowell
Rose and Milton Friedman
Senior Fellow in Public Policy
Hoover Institution
Stanford University

Murray L. Weidenbaum
Mallinckrodt Distinguished
University Professor
Washington University

Richard J. Zeckhauser
Frank Plumpton Ramsey Professor
of Political Economy
Kennedy School of Government
Harvard University

Research Staff

Joseph R. Antos
Resident Scholar

Leon Aron
Resident Scholar

Claude E. Barfield
Resident Scholar, Director, Science
and Technology Policy Studies

Walter Berns
Resident Scholar

Douglas J. Besharov
Joseph J. and Violet Jacobs
Scholar in Social Welfare Studies

Robert H. Bork
Senior Fellow

Karlyn H. Bowman
Resident Fellow

Montgomery Brown
Director of Publications

John E. Calfee
Resident Scholar

Charles W. Calomiris
Visiting Scholar

Lynne V. Cheney
Senior Fellow

Nicholas Eberstadt
Henry Wendt Scholar in Political
Economy

Mark Falcoff
Resident Scholar

J. Michael Finger
Resident Fellow

Gerald R. Ford
Distinguished Fellow

Murray F. Foss
Visiting Scholar

Hillel Fradkin
W. H. Brady, Jr. Fellow

Harold Furchtgott-Roth
Visiting Fellow

Jeffrey Gedmin
Resident Scholar, Executive
Director, New Atlantic Initiative

Newt Gingrich
Senior Fellow

James K. Glassman
Resident Fellow

Robert A. Goldwin
Resident Scholar

Michael S. Greve
John G. Searle Scholar

Robert W. Hahn
Resident Scholar, Director,
AEI-Brookings Joint Center
for Regulatory Studies

Kevin A. Hassett
Resident Scholar

Thomas W. Hazlett
Resident Scholar

Robert B. Helms
Resident Scholar, Director, Health
Policy Studies

James D. Johnston
Resident Fellow

Jeane J. Kirkpatrick
Senior Fellow, Director, Foreign and
Defense Policy Studies

Marvin H. Kosters
Resident Scholar, Director,
Economic Policy Studies

Irving Kristol
Senior Fellow

Michael A. Ledeen
Freedom Scholar

James R. Lilley
Resident Fellow

John R. Lott, Jr.
Resident Scholar

Randall Lutter
Resident Scholar

John H. Makin
Resident Scholar, Director,
Fiscal Policy Studies

Allan H. Meltzer
Visiting Scholar

Joshua Muravchik
Resident Scholar

Charles Murray
Bradley Fellow

Michael Novak
George Frederick Jewett Scholar
in Religion, Philosophy, and Public
Policy, Director, Social and Political
Studies

Norman J. Ornstein
Resident Scholar

Richard N. Perle
Resident Fellow

Sarath Rajapatirana
Visiting Scholar

Sally Satel
W. H. Brady, Jr. Fellow

William Schneider
Resident Fellow

J. Gregory Sidak
F. K. Weyerhaeuser Fellow in Law
and Economics

Christina Hoff Sommers
Resident Scholar

Daniel E. Troy
Associate Scholar

Arthur Waldron
Visiting Scholar, Director, Asian
Studies

Graham Walker
Visiting Scholar

Peter J. Wallison
Resident Fellow

Ben J. Wattenberg
Senior Fellow

David Wurmser
Research Fellow

Karl Zinsmeister
J. B. Fuqua Fellow, Editor,
The American Enterprise