

FOREIGN AFFAIRS

NOVEMBER / DECEMBER 2009



Losing Controls

How U.S. Export Restrictions Jeopardize
National Security and Harm Competitiveness

Mitchel B. Wallerstein

Volume 88 • Number 6

The contents of *Foreign Affairs* are copyrighted. ©2009 Council on Foreign Relations, Inc. All rights reserved. Reproduction and distribution of this material is permitted only with the express written consent of *Foreign Affairs*. Visit www.foreignaffairs.org/permissions for more information.

Losing Controls

How U.S. Export Restrictions Jeopardize National Security and Harm Competitiveness

Mitchel B. Wallerstein

Since the early days of the Cold War, the United States has restricted the export of certain advanced technologies and the sharing of sensitive scientific and technical information with foreign nationals. Initially, these restrictions were justified on the grounds that the Soviet Union and its Warsaw Pact allies were engaged—through fronts, third parties, and outright espionage—in a systematic effort to buy or steal information, technology, and equipment developed in the West that they could then use in their own military systems. Because Soviet industry could not design or produce certain high-tech products, such as personal computers or sophisticated machine tools, the Soviets were forced to obtain them by other means. By successfully denying technology to the Soviet Union, the United States enabled NATO to maintain a strategic and tactical advantage without having to match the Warsaw Pact nations' troop strength in the field. Yet 20 years after the fall of the Berlin

Wall and long after the Soviet Union ceased to exist, the same system of export controls remains in place. It has only become more arcane and ineffective with time.

U.S. export controls have survived largely because of outdated “fortress America” thinking—the view that the United States is the primary source of most militarily useful scientific ideas and products and that it can continue to deny technology to potential adversaries without seriously damaging the global competitiveness of U.S. companies or, in the end, jeopardizing national security. In an earlier era, when the United States was far more economically and technologically dominant, the costs associated with a technology-denial strategy were easier to absorb. But in today's highly competitive world, the business lost due to export controls poses a threat to the well-being of key U.S. industries; estimated losses range as high as \$9 billion per year.

MITCHEL B. WALLERSTEIN is Dean of the Maxwell School of Syracuse University. He was U.S. Deputy Assistant Secretary of Defense for Counterproliferation Policy and Senior Defense Representative for Trade Security Policy from 1993 to 1997.

OUT OF CONTROL

In the early 1990s, after the breakup of the Soviet Union, it became increasingly clear that the United States, its NATO allies, and Japan no longer saw eye to eye when it came to sustaining a far-reaching system of export restrictions. Having lost this consensus, it became inevitable that the informal Cold War-era organization known as the Coordinating Committee on Multilateral Export Controls (CoCom) would be dissolved. With the former CoCom countries threatening to go their separate ways, the United States, which had long served as the principal driver of multilateral export controls, launched a diplomatic initiative in 1994 to negotiate a successor regime that would also include Russia, Ukraine, and other key eastern European states as members.

It soon became apparent, however, that there was little possibility of establishing a new regime similar to CoCom. Washington settled for a far less comprehensive agreement, the Wassenaar Arrangement, which was concluded in the Netherlands in 1996. It neither requires member states to consult with one another prior to approving an export nor permits one member state to block an export by another on security grounds, as was the case under CoCom. Predictably, the Wassenaar Arrangement has achieved only minimal success as a technology-denial regime.

Most technologically advanced countries saw the end of the Cold War as an opportunity to end restrictions on the export of all but the most highly sensitive technology and information, such as nuclear technology and designs, biological agents and equipment, or long-range missiles. In their view, export controls could no

longer be effective in a world where information moves electronically and computers and other dual-use technologies—products or parts that are developed and manufactured by the private sector for both military and commercial applications—have become commodities. Indeed, the very notion of “militarily significant technology” has in some respects lost its meaning, given that the computational power needed to perform many military applications is now far below the standard performance levels of widely available personal computers, most of which are manufactured outside the United States.

Because the European states are inclined to view technology denial as a largely outdated policy instrument, they have not been motivated to establish a coherent EU-wide policy on export controls. Instead, they continue to maintain a loose system of nationally based controls on dual-use technologies. And arms exports remain entirely subject to national discretion, guided only by a nonbinding EU “code of conduct.”

The loss of multilateral consensus on the need for controls has been coupled with more than a decade of policy paralysis and political stalemate within the United States. During the George W. Bush administration—and especially after 9/11, the invasion of Iraq, and North Korea’s nuclear and missile tests—conservative forces in the White House and the Pentagon actively resisted most ideas circulated within the administration for modifying U.S. export control policy: changes that might have aligned the United States more closely with the positions of other technologically advanced states. Although the Bush administration’s refusal to address export control reform was driven primarily

Losing Controls

by ideology, it also reflected an understandable desire not to send the wrong signal to terrorist groups or potential proliferators.

As in the executive branch, gridlock has reigned in Congress when it comes to export control policy, pitting those who remain invested in “fortress America” thinking against those pressing for a more rational system based on the economic and technological realities of the twenty-first century. The Export Administration Act, which is the principal law governing dual-use exports, lapsed in 2001 after 12 unsuccessful attempts since 1990 to modify and reauthorize it. As a result, successive presidents have been forced to invoke the authority granted under the International Economic Emergency Powers Act of 1977 to maintain export regulations.

There have recently been some hopeful signs from both the White House and Congress that the policy logjam might finally be breaking. President Barack Obama has announced a full-scale inter-agency review of U.S. export control policy. And Congressman Howard Berman (D-Calif.), chair of the House Foreign Affairs Committee, has indicated that he intends to introduce new legislation during this session of Congress to modify and renew the Export Administration Act. Until such changes are implemented, the country’s security and economic competitiveness will remain threatened.

LESS COMPETITIVE, LESS SECURE

Export controls undermine national security in at least four ways. First, the majority of the most important technologies incorporated into U.S. military systems are today inherently dual-use. But some U.S. high-tech firms believe—often erroneously—that they can avoid the financial costs and

legal restrictions associated with export controls by choosing to invest in technologies with no apparent military applications. This has the effect of depriving the Defense Department of cutting-edge products, as well as access to the fruits of some of the most innovative technology developers in the United States. Small start-up firms are particularly unable and unwilling to tolerate the risk and expense associated with long export-licensing delays.

Second, foreign manufacturers who may in some cases possess more advanced technology than rival U.S. companies often choose not to compete for U.S. defense contracts out of a similar fear of becoming entangled in U.S. export controls. In the case of the multinational Joint Strike Fighter program, in which some of the most innovative subsystems were engineered by non-U.S. companies, the U.S. export control system has created so many difficulties that the British government actually threatened to cancel its participation in the program.

Third, the U.S. military is sometimes unable to outsource the repair and maintenance of its equipment to foreign companies in allied countries—which are often much closer to the battlefield—because doing so would require individual export licenses for each piece of equipment serviced.

Finally, export restrictions can degrade the ability of U.S. defense attachés and intelligence officials to obtain important knowledge of foreign military capabilities and scientific and technological developments. When U.S. companies are involved in foreign sales or cooperative production agreements, there is typically some sharing of technical data and information that can help them learn about the capabilities of foreign militaries. When they are not,

the U.S. government cannot obtain this valuable military and technical intelligence.

Concerns about the impact of export controls extend well beyond the realm of national security; business leaders have spoken out for decades about the economic price of these outmoded laws and regulations. Senior executives from companies in sectors as diverse as computers (Hewlett-Packard and IBM), communications satellites (Hughes, now Boeing), aerospace (United Technologies), and machine tools (MAG Industrial Automation Systems) have voiced concerns about the uneven playing field created by overreaching U.S. controls, which impose licensing requirements that foreign competitors do not face. Hardliners both within and outside the U.S. government have generally dismissed such concerns, arguing that they merely represent self-interested behavior on the part of U.S. firms. Yet as the Cold War has faded into history and as the global economic position of U.S. companies has declined relative to foreign competition, these industry concerns have become increasingly compelling.

In today's highly integrated global markets, where research and development (R & D) and production capabilities are far more widely distributed, the continuation of a comprehensive system of export controls harms U.S. competitiveness in a number of ways. First, controls impose compliance requirements on U.S. firms that increase their costs of doing business relative to the costs of their foreign competitors.

Second, U.S. components are, in some cases, being intentionally designed out of systems manufactured abroad so that the manufacturing companies avoid having to subject specific components to U.S. export control laws. There is also evidence that the constraining effect of U.S. regulations

has created a market niche for foreign competitors in the areas of aerospace (the European Aeronautic Defence and Space Company), satellites (Thales Alenia Space), composite carbon manufacturing equipment (the Spanish firm M. Torres), and Night Vision equipment (which is produced by numerous firms in France, Israel, South Africa, and even China and Russia). In some situations, foreign competitors have stepped in to meet the demand—often with the active support of their governments. Certain foreign companies, such as the satellite manufacturer Thales Alenia Space and the rocket motor manufacturer Swiss Propulsion Laboratory, actually advertise that their products are totally free of U.S. content. The European space industry now explicitly claims to be an “ITAR-free zone,” meaning that its companies and products do not utilize U.S. content that would be subject to the International Traffic in Arms Regulations implemented under the U.S. Arms Export Control Act.

Third, U.S. firms that maintain R & D facilities in foreign countries, as many now do, are forced to compartmentalize access to information so that employees who are not U.S. citizens do not have access to technical data and other information that is subject to U.S. export controls. (Similar procedures are also imposed at domestic R & D facilities where foreign nationals are employed.) The net effect of these restrictions has been to deprive U.S. companies of some of the best and brightest scientists and engineers in the world—people who could spearhead the next generation of technological advances.

This same phenomenon also lessens the ability of U.S. universities—many of which conduct defense research on contract for major corporations or the U.S.

Losing Controls

government—to recruit and retain foreign scientists and engineers. The U.S. university R & D infrastructure has long been the envy of the world, and it is today highly reliant on noncitizens (in large part because the United States is not producing sufficient numbers of scientists and engineers).

After 9/11, many foreign experts decided that they did not wish to be subjected to visa interview requirements, special scrutiny and biometric scans at the U.S. border, visa controls that limited where they could travel in the United States or how long they could stay, or rules that prevented them from seeing or discussing certain categories of technical information (because under U.S. regulations, the disclosure of such information to foreigners is deemed tantamount to exporting it). Many are instead taking advantage of the growing number of attractive opportunities at European, Asian, and Australian universities. Here, as well, “fortress America” thinking is depriving the United States of the very people it needs to remain at the cutting edge of science and technology.

The United States has been a magnet for foreign scientific talent since at least the 1930s, when a number of eminent Jewish scientists and those married to Jews were forced to emigrate from Europe in large numbers. Many of these individuals—most famously, Albert Einstein and Enrico Fermi—made enormous contributions to the U.S. war effort during World War II. Turning away foreign talent today is self-defeating, and such policies threaten the future viability of the country’s high-tech economy and, ultimately, its national security.

DISMANTLING THE FORTRESS

Several scenarios are often identified by those favoring the continuation of export

restrictions: the military resurgence of Russia; the rise of China as a military power; an increase in threats from “rogue states,” such as Iran and North Korea; and the possibility that a terrorist group might acquire the know-how, weapons designs, and components needed to construct one or more mass-casualty weapons. Each of these cases is unique, and each demands a tailored policy response.

Few experts believe that Russia has either the resources or the inclination to reconstitute a serious military threat to Europe, even though it has recently demonstrated its capacity to threaten its smaller southern neighbors. As President Obama reiterated during his June visit to Moscow, Russia is no longer an enemy, and part of the effort to “reset” the U.S.-Russian relationship depends on encouraging a two-way flow of people, ideas, and technology. A continued technology-denial approach in this case not only would be inimical to the effort to improve U.S.-Russian relations but also would be largely pointless given that Russia has equal mastery of nuclear and biological weapons and now has largely unfettered access to computers and most other militarily applicable dual-use technologies.

In the case of China, the argument for retaining export restrictions on certain types of information and sensitive technology is somewhat more persuasive given that China appears to be a rising military competitor with unclear regional ambitions. At the same time, in view of the economic interdependency between China and the United States and China’s increasing investment in domestic R & D and advanced manufacturing operations, Washington may soon lose its ability to deny certain technologies to Beijing anyway.

It may be smarter in the long run to encourage U.S. high-tech firms to engage more deeply in China, with the exception of providing direct support to the Chinese military industry or the People's Liberation Army. Given that it is often difficult to monitor scientific and technological developments in the traditionally closed Chinese society, such expanded engagement is likely to increase transparency and lead to even greater interdependence, a situation that would likely benefit the United States more than China.

The United States has done this before. Washington deepened its engagement with Beijing during the 1990s, albeit somewhat inadvertently, when the Clinton administration permitted the launch of some U.S. commercial satellites on Chinese rockets. After a series of launch failures, engineers from the U.S. satellite manufacturers were invited to consult with their Chinese counterparts in order to fix the problem. But this consultation did not sit well with some in the U.S. government, who feared that such technical assistance might help the Chinese improve the reliability of their intercontinental ballistic missile systems. Congress established an investigative body (known as the Cox Commission) to review the matter and ultimately mandated that all satellites should be reclassified as munitions—henceforth to be regulated by the State Department under the Arms Export Control Act. This effectively ended U.S.-Chinese technical cooperation on commercial satellite launches. Although Congress was right that there is little distinction, from a technological standpoint, between commercial and military space launch vehicles, Washington's decision to end cooperation with Beijing had the

unfortunate side effect of shutting down an important channel that could have enabled the United States to gain knowledge of Chinese missile designs and launch capabilities.

Carefully targeted export controls unquestionably remain necessary with respect to states that are known to be or are suspected of seeking mass-casualty weapons or new and expanded military capabilities that could threaten neighboring countries. It is established, for example, that both Iran and North Korea have actively and successfully shopped world markets for specific technologies—such as high-speed centrifuges—and both reportedly were clients of the Pakistani scientist A. Q. Khan's now-defunct nuclear proliferation network. There are also allegations that technical experts from North Korea helped Syria build the secret nuclear facility that was destroyed by Israel in 2007. Given the UN Security Council's sanctions against both Iran and North Korea, the prospects for continued multilateral cooperation on denying sensitive technology to these countries appear reasonably good, at least in the near term. In the longer term, however, like-minded states will need to support UN sanctions and apply nationally based controls in a more effective and coordinated fashion as one way of encouraging proliferators to abandon their nuclear and biological weapons programs.

The effort to deny terrorists access to technology and sensitive information about mass-casualty weapons remains the most difficult challenge of all. It is worth bearing in mind, however, that terrorist organizations do not currently have enough money or technical know-how to operate their own weapons research

or manufacturing facilities. Rather, they are focused on trying to buy or steal weapons or the fissile material, biological agents, and other key components needed to construct one. Sweeping export controls—even those that are enforced multilaterally—may simply be too imprecise a policy instrument to be effective against determined terrorist groups. Much more important are efforts to deprive terrorists of the technical know-how they need to assemble, transport, and detonate a mass-casualty weapon. Successful technology denial in this case requires, among other things, close cooperation among intelligence services in vigilantly monitoring scientists—and, when necessary, intervening—to stop future A. Q. Khans when there is evidence that they are providing or seeking to provide weapons information or material support to terrorists.

CONTROLS THAT WORK

“Fortress America” thinking is dangerously out of touch with today’s global economic and technological realities. The United States’ indiscriminate use of export controls means that government resources are wasted on compliance efforts that do not make the country any safer. This, in turn, makes it difficult to focus on the limited number of controls—such as restricting transfers of nuclear components—that actually can enhance national security.

Much has changed in the two decades since the end of the Cold War. The United States has not declined economically or technologically, but other countries have caught up. They are now producing advanced technology that is in many cases equal to or better than that designed and manufactured in the United States. Most militarily applicable technology is now

dual-use in nature, and the majority of it is not subject to control by any nation other than the United States. This means that unilateral U.S. control efforts will only work in a limited number of situations—namely, those in which the United States either is the sole supplier or enjoys overwhelming market dominance. Stealth technology, very high-resolution satellites, and encryption software are among the few remaining areas in which the United States still enjoys such an advantage.

As a recent study by the National Research Council's Committee on Science, Security, and Prosperity concluded, U.S. policy should impose restrictions only in those cases in which the United States and its allies possess technology that provides an identifiable military advantage that is likely to persist for a significant period of time, the United States and its allies control the technology and can prevent its transfer to potential adversaries, and the restrictions will not impose costs and inefficiencies that are disproportionate to the security benefits achieved. In addition, the viability of any restrictions imposed should be reconsidered on a regular basis as technologies age and market conditions change.

The current approach of the U.S. government to the administration of export controls fails to adhere to these criteria. Still mired in the risk-averse thinking of the Cold War, policymakers in multiple government agencies continue to maintain long lists of obsolescent technologies that are still subject to controls and continue to support barring the export of products that are often widely available outside the United States. Indeed, in many cases, those responsible for making the technical judgments about which

technologies and scientific information should be subject to control lack the necessary advanced training and state-of-the-art knowledge—expertise that can only be derived from direct involvement in the R & D process in the universities and industries in which these technologies are being developed.

Under specific circumstances, export controls remain a necessary and useful instrument of U.S. policy. But policymakers must abandon the notion that the United States can still be a fortress and that it can engage in technology denial without suffering significant costs to its prosperity and national security. Unless export controls are more narrowly defined and carefully targeted, they will increasingly do more harm than good. 🌐