Computer Exports and National Security in a Global Era

James A. Lewis
CSIS
June 2001
Introduction

The Center for Strategic and International Studies (CSIS) has carried out a comprehensive analysis of how the United States should reform export controls for information technology. CSIS established a Senior Commission and three working groups to assess the current export control framework and consider changes in policies and procedures that would strengthen national security (see appendix B for the list of commission and working group members). The goal was to find practical policy recommendations. This volume, *Computer Exports and National Security in a Global Era: New Tools for a New Century*, grows out of the work of these experts and provides an overview of the issue and recommendations on how to move forward.

Export controls on computers and microprocessors have been a politically charged subject for much of the past decade. *Computer Exports and National Security in a Global Era* reaches three broad conclusions: (1) Current export controls on computers and microprocessors are ineffective, given the global diffusion of information technology and rapid increases in performance. (2) The United States should eliminate these Cold War controls and strengthen military and proliferation-related controls. (3) The trends that make computer export controls ineffective could damage national security if the United States does not use new information technologies to retain its military advantage over potential opponents.

The study is divided into four chapters: A New Context for Controls; Proliferation and Cooperation; Multilateral Cooperation on Export Controls; and Computer Technology and National Security. The underlying theme of these chapters is that export controls must adjust to fundamental changes that have occurred in the world since 1991, when the Cold War export regime—the Coordinating Committee for Multilateral Export Controls or CoCom—laid the foundation for computer export controls. The most important of these changes are political and technological. The Cold War’s end removed political obstacles to global economic integration. It also eroded consensus among the United States and its allies on how to control exports of commercial products like computers. Technologically, the stupendous increase in performance and the growth of the Internet means that computing power is increasingly ubiquitous.

These changes are well known. What this study does is connect them to draw conclusions for export controls. If computing power greater than that used to build the most sophisticated weapons is now widely available, if there is no consensus among allies to restrict access to this computing power, export control policy needs significant restructuring. The issue for restructuring is whether the United States retains the ability to deny potential opponents or proliferators’ access to the computing power they need for military purposes. After measuring the availability of computing power and the amount needed for military purposes, this report concludes that the United States no longer has this ability.

As might be expected, access can be controlled for technologies that are relatively costly, made by few manufacturers, have few substitutes, and are sold in specialized markets for specialized
purposes. This was once true of computers but is no longer the case. Computers are now relatively cheap, made by many manufacturers, and sold in a global market, making it easy to obtain computing power. Chapter 1 details increases in microprocessor performance that make a single inexpensive chip more powerful than the supercomputers used to design modern U.S. weapons. It also looks at how the Internet has increased access to high performance computing by fueling demand for computers, with more than 130 million units sold worldwide last year, and by enabling the connectivity that lets networks of ordinary computer provide “supercomputing” levels of performance.

Chapter 2 concludes that the public debate has overestimated the amount of computing power needed for military and weapons purposes. Ordinary desktop computers and workstations can meet military requirements if—and this is the crucial element—they are running the necessary software and databases. Export controls need to concentrate on what is essential (the software) and not seek to control hardware that grows exponentially in capability and is sold in the tens of millions of units worldwide every year.

Chapter 3 reviews the status of multilateral cooperation. The Wassenaar Arrangement controls computers and general-purpose microprocessors. Its weaknesses are well documented, most recently in a joint Stimson Center/CSIS report. Calling for strengthened multilateral controls on information technology would be easy, but chapter 3 concludes that such a recommendation cannot be implemented, given the difficulties in controlling computers and microprocessors, the lack of a clear strategic or nonproliferation rationale, and the frustration felt by U.S. allies over computer controls.

Chapter 4 looks at ideas that would allow the United States to take advantage of information technology to preserve its military advantage over potential opponents. It recommends closer cooperation between the private sector and government, changes in acquisitions processes, and a strengthening of education and research and development.

The report contains a series of recommendations for strengthening U.S. national security that fall into three groups: ending Cold War export controls, strengthening proliferation-related controls, and accelerating the process by which the United States gains national security advantage from information technology. Implementing these recommendations may be difficult, but national security will improve once the United States embarks on a path of reform.
Contents

Introduction i
Table of Contents iv
Executive Summary v

Performance Improvements and Increased Access to Computational Power v
Information Technology and Proliferation vi
Multilateral Cooperation on Export Controls vii
MTOPS No Longer Works viii
Export Controls After MTOPS viii
Effect on National Security ix
Preserving Military Superiority ix

Recommendations

A New Context for Controls 1
Computer Exports and National Security in a Global Era 1
Sell Globally or Go Bankrupt Locally 3
Performance and Technological Improvement 5
Access to Computing Power 8
Conclusion 11

Proliferation and Cooperation 13
Conclusion 17

Multilateral Cooperation on Export Controls 18
The Question of MTOPS 21
The Effect on U.S. National Security 22
Post-CoCom Export Controls 24

Computer Technology and National Security 29
Education, Research and Development 32

Appendix A - MTOPS and Its Alternatives 37
Executive Summary

The United States faces complex challenges in a world that has changed significantly since the 1980s. Intractable regional conflicts, terrorism, and the proliferation of weapons of mass destruction threaten U.S. national interests. The inexorable spread of information and technology throughout an increasingly competitive world marketplace create new challenges for U.S. security.

Export controls on information technology derive from an era when the strategy of the United States and its allies was to deny technology to the Soviet Union and keep the Western alliance strong. Trade, communication, and cooperation between the two sides of this conflict were limited. Allied cooperation, and the very real threat posed by the Soviets, made technology embargoes and economic warfare effective. This is no longer the case.

The collapse of the Soviet Union removed the single largest obstacle to increased economic integration. Technological change has reinforced economic integration. Improved telecommunications, transportation, and the creation of the Internet allow rapid, cheap, and accurate transfers of information. In combination, these changes in telecommunications, air travel, and shipping have created unprecedented mobility of goods, people, and ideas.

Fewer obstacles to international trade mean that industries are increasingly integrated along lines of lowest cost rather than national borders. Research and manufacturing for information technology are global. Access to technology and technical capabilities have spread widely and continue to spread across a global market. The United States leads in many of these technologies, but it does not have a monopoly. Barriers to entry for new competitors in the information technology market tend to be economic rather than technological—the question is not whether they can build a product, but whether they can make money selling it.

Performance Improvements and Increased Access to Computational Power

Computing power is becoming ubiquitous, as more and more devices contain processing capabilities equal to what was once considered a supercomputer. There are many ways to obtain access to high performance computing without a high performance computer. Increases in microprocessor performance are the key to understanding the increase in access to computing power. These increases are the result of steady improvements in the chip manufacturing process. The microprocessor “brain” of computers has gone from 12 MTOPS to 4000 MTOPS in a decade (MTOPS is a measure of speed and performance). Software that allows commodity computers to be clustered with low-level commercial “interconnect” technologies to provide high performance computing allows universities and research centers to
draw upon the installed base of tens of millions of desktop computer as the raw material for supercomputing.

Supercomputer performance shows a similar trend. Twenty years ago, “supercomputers” performed at a few hundred MTOPS. Today, the most powerful computers operate in the millions of MTOPS. Companies, universities, and research institutions around the world can now assemble powerful computers from uncontrolled commercial components and software.

Access to computational power continues to expand because of the Internet. Some companies have begun to use the Internet to combine hundreds or even thousands of desktop computers in widely separated locations into a single computing system. The next generation Internet, with its greater “bandwidth” (the amount of data that a network can carry), will make access to high performance computing even easier. Computer export controls pre-date these widely available techniques for high performance computing. Efforts to control them would fail in the face of their simplicity and the widespread availability of the necessary hardware.

**Information Technology and Proliferation**

Critics of increased control thresholds believe that high performance computers are a particularly sensitive “enabling” technology for nuclear weapons, missiles, submarines, and other military applications. It seems reasonable to assume that if computers and microprocessors are the engines of economic growth that they are also engines of military strength, but this assumption is wrong. The dramatic increase in computing power over the past 10 years and the transformation of computers from highly specialized research tools into a network commodity break the connection between high performance computing and weapons proliferation.

Military applications do not require much computing power. This is especially true for weapons design and manufacturing. The United States designed and built its weapons with computers of 500 to 1000 MTOPS. At the time, these were large, sophisticated supercomputers. High performance computers as we know them today did not exist. Low-level systems can now provide the computing power once supplied only by these “supercomputers.” For example, the F-22, the most advanced U.S. fighter, was designed with a 958 MTOPS Cray supercomputer, roughly one-quarter of the power found in mass-produced Pentium chips. Computing power is considerably less important for building modern weapons than is the ability to integrate materials, manufacturing equipment, and technology. This ability to integrate disparate
technologies requires years of experience, not powerful computers.

Computational power is also of little benefit for weapons design unless the computer is running sophisticated codes based on extensive experience and test data. For nuclear weapons design, a central concern in the computer export debate, access to data derived from nuclear weapons explosions is more important than computing power. A country without extensive experience in weapons design is at a significant disadvantage, and the lack of reliable data and proven codes will substantially constrain the usefulness of computer technology for military or proliferation purposes.

A key objective of the Cold War’s export control system was to prevent the Soviet Union from using Western-made microprocessors and computers as components in weapons systems or for battle-management purposes such as air defense, antisubmarine warfare, battle management, and weather prediction. This objective lives on in export controls despite radical changes in the international security and economic environment.

Again, performance increases have undercut efforts at denial. Desktop computers, workstations, and servers can perform many battlefield applications, and the trend in commercial technology has been to use small powerful devices to provide the range of mobile applications. The United States itself used elderly 650 MTOPS VAX computers until recently in the J-STARS battlefield surveillance aircraft. EP-3E aircraft, the type involved in the recent incident in China, used 240 MTOPS workstations. Retail laptops are more powerful than this. For these military applications, as for design and manufacture, computing power is less critical than the ability to integrate computers, sensors, and platforms into an effective system. The U.S. lead in military software and in fielding advanced space-based and aircraft sensors limits the ability of any potential opponent to compete with the United States solely on the basis of access to computer hardware.

Microprocessor performance increases combined with software developments that allow for clustered computers mean that today’s low-level systems provide all the computing power needed for military and proliferation-related applications. Technological improvements have eroded the proliferation and security rationale for control. One result of these changes has been a marked reduction in allied support for controls on information technology.

**Multilateral Cooperation on Export Controls**

Multilateral cooperation in controlling information technologies is at a low ebb, primarily because there is no convincing strategic or nonproliferation rationale for continued control. Missteps by the United States in coordinating computer controls with its partners have also reduced the scope of cooperation. This is particularly true for Japan, where a formal obligation by the United States to consult in advance of any change in computer controls was often observed in the breach.

The multilateral nonproliferation regimes (the Nuclear Suppliers Group, Missile Technology Control Regime, and Australia Group) do not control computers. The Wassenaar Arrangement, which does control computers, is by any measure less effective than its nonproliferation
counterparts. Wassenaar computer controls are set at a level far above what most military applications need, and the regime has been decontrolling information technology since its inception. Wassenaar members will not embargo civil technology to countries like China or India. Consensus between the United States and its allies on potential threats and on technology transfer has eroded, and the combination of a lack of a common security threat and the emergence of a competitive global market means that there is no multilateral support for Cold War–style economic warfare or embargo.

Similar problems dog the bilateral supercomputer regime the United States created with Japan in the 1980s. The bilateral arrangement involved a prior consultation process, whereby each country would notify the other before approving the export of a supercomputer, and an agreed set of conditions and safeguards that each country would apply to exports. Over time, poor coordination and the lack of a strategic rationale have damaged the bilateral regime. Japan has asked to terminate the bilateral computer agreement.

The United States has blocked change in Wassenaar for several years. This effort has not prevented computing power from spreading around the globe. A better strategy would be to try to use the rationalization of computer and microprocessor controls in Wassenaar as leverage to refocus the regime on sensitive technologies that can still be controlled.

**MTOPS No Longer Works**

MTOPS, a measure of computer speed created in the early 1990s, is the core of CoCom-based controls. It is an artificial construct used solely for export control purposes. The MTOPS metric has come under pressure as performance increases in the past five years forced the United States to choose between raising control levels or licensing millions of commodity-level computers. Government and industry have explored several alternatives to MTOPS—none have been satisfactory. MTOPS cannot accurately measure performance of current microprocessors or alternative sources of supercomputing like clustering. This makes MTOPS-based hardware controls irrelevant, a trend reinforced by the lack of multilateral cooperation and the continued increases in computing power. The best choice may be to simply eliminate MTOPS.

**Export Controls after MTOPS**

Three sets of controls will still apply to exports of information technologies if the United States ends CoCom-era controls. Sanctions will apply to exports to countries like Iran. Munitions controls will apply to systems and software specially developed for military purposes. The U.S. Department of Defense (DOD) recommends that munitions controls focus on critical national security applications developed specifically for the military and that the United States seek additional ways (such as encryption-based software protection) to safeguard these applications.

The chief authority that the United States will have for controlling information technology hardware would be the U.S. “catch-all” control known as the Enhanced Proliferation Control Initiative (EPCI). EPCI controls will continue to allow the United States to stop U.S. firms from exporting information technologies at all performance levels to proliferators without the need for
MTOPS-based controls.

The EPCI process that has developed over the past decade could do better at supplying information about proliferators from the government to the private sector. One step would be to expand the “Entity List” used by the United States to warn exporters not to sell to certain customers. It currently lists perhaps 10 percent of proliferation-related entities. An expanded “is informed” process is also necessary. When one exporter “is informed” that there are proliferation concerns with a potential customer, all known potential exporters should be informed. The “is informed” process could also take advantage of Web-based technologies to provide a greater flow of information. Companies could improve their screening of potential buyers if the United States used lists of items and countries focused on real proliferation concerns. The United States could focus the list of countries that require screening onto those places where there are proliferation concerns. Strengthening EPCI requires a more focused approach to entities and technologies and a greater effort to share information on proliferation-related entities as broadly as possible.

**Effect on National Security**

The widespread availability of computing power is part of a larger trend identified by the Defense Science Board Task Force on Globalization—the global diffusion of military technologies and the availability and rapid pace of development in commercial technologies. This trend could degrade national security unless the United States takes effective steps in response.

Many potential adversaries realize that greater access to technology can provide them with advantages. Their military goals are not to achieve strategic parity with the United States, but instead to gain the ability to disrupt or deny the United States its power projection capabilities that allow it to insert a rapid and powerful military presence in their region. At the same time, the size and development of U.S. forces and its high-tech economy give it an advantage over opponents in exploiting information technologies. No other nation has the range of military capabilities that the United States possesses and will gain as much from integrating information technology into military operations. Unique U.S. software applications based on years of operational experience and extensive testing provide considerable advantage. A new policy for information technology should focus on strengthening controls on this software and seeking to extend U.S. advantage by developing specialized new military software applications.

**Preserving Military Superiority**

Military power today depends not only on the tools of the industrial age but on the tools of the information age as well. The Defense Department can no longer depend on a dedicated defense-industrial base, but will need to find ways to link advanced commercial technologies to improved military capabilities. The United States needs new ways to work with the private sector to enhance U.S. security. Potential opponents will seek to exploit U.S. vulnerabilities with the new technologies. For the United States, information technology, properly integrated into battlefield operations, can provide the margin of victory.
Many efforts are under way in the United States and in foreign countries to use information 
technologies in military operations. If a global economy makes denying access to these 
technologies ineffective, the United States must reap greater benefit from them than can its 
potential opponents. Maintaining U.S. superiority requires building closer partnerships with the 
information technology industry and academic community; creating a process to increase the 
flow of innovation and to change doctrine and practices accordingly; and taking the steps needed 
to build a strong foundation of education and research to ensure that U.S. technology is as 
advanced in 10 years as it is today.

Vehicles for partnership include new advisory groups, task forces, exchange programs for 
Defense Department personnel at information technology companies, internships, and the 
establishment of joint research programs. The broad objective should be to create interfaces 
between the government and the private sector that match warfighters’ needs and private sector 
innovations. Partnership initiatives could include the creation of a joint evaluation center to look 
at technologies and applications. The United States could expand existing activities at the 
National Defense University and other military education facilities by adding programs and 
faculty staffed by technologists from information technologies industries.

Adopting B2B (business-to-business) models would streamline acquisitions activities. The 
creation of a business-to-business portal by the General Motors Corporation, Ford Motor 
Company, and DaimlerChrysler is a useful model for Defense. Improved logistics and 
aquisitions can help the Defense Department upgrade its information technology. Using old 
technology can be expensive, as models go out of production and spare parts and maintenance 
costs increase. B2B practices would allow DOD and the armed services to have a faster “refresh 
rate” for information technology. Congress and the administration will need to change the 
aquisitions process for the United States to gain the full benefit of its lead in commercial 
technologies.

The United States can capitalize on private sector experience with integrating information 
technology. DOD or the Defense Advanced Research Projects Agency (DARPA) might wish to 
begin four or five fast-track programs with leading information technology companies to develop 
new applications. Possible fast-track program areas include wireless broadband applications, 
pervasive computing, embedded intelligence applications, software agents, data mining, other 
automatic database applications and collaborative virtual workspaces.

Potential opponents will also face a more difficult task if the United States improves its 
information security. To some extent, this is a question of making encryption an integral part of 
national security applications and strengthening critical infrastructure protection and information 
assurance efforts. The United States needs to ensure that its cyberspace capabilities match the 
capabilities of conventional forces.

Enhancing national security with new information technology also requires strengthening 
education and long-term research and development. The United States needs incentives and 
programs that will produce an adequate supply of information technologists. One solution might
be to use scholarships where the United States would pay for higher education in exchange for a commitment to service for a number of years, as is already done with other short-supply skills such as medical care. Funding research and development in new technologies is also crucial. If the pipeline of innovation runs dry, the United States would lose an important element of its superiority. This expansion should apply to research both in information technologies and in basic research.

Denying access to computing power was strategically important in the 1980s, but now the United States needs to recast the issue. A new administration and new Congress have the opportunity to take bold, necessary steps to advance U.S. national security. To that end, the following recommendations are presented.

**Recommendations**

**End CoCom Controls.** Given the global market in computers and computer components, the widespread availability of substitutes for controlled hardware, and the low level of computing needed for almost all military or weapons related tasks, the hardware controls that originated in CoCom no longer make sense. The computational capability needed for military or proliferation purposes (1000 MTOPS or less) has been outside the bounds of control since 1993. Eliminating CoCom-based hardware controls also eliminates the problem of how to replace MTOPS—a metric that is now obsolete for the technology it seeks to control.

- The National Security Council (NSC) and appropriate agencies should develop a legislative strategy for changes in law needed to eliminate MTOPS-based controls.
- Congress should repeal or amend existing legislation to eliminate any requirements for the use of MTOPS-based controls.
- The Department of Commerce should also to identify and implement necessary regulatory changes to eliminate MTOPS-based controls inherited from CoCom from existing dual-use regulations.
- In concert with these actions, the Department of State should take the necessary steps to win other nations’ support for elimination of MTOPS-based controls in the Wassenaar Arrangement and be prepared to escalate the matter to senior-level attention in Wassenaar countries to counter any mischievous action.
- The Department of State should also work with Japan to terminate the bilateral supercomputer arrangement in a way that allows Japan to continue to meet its nonproliferation commitments.

**Strengthen EPCI.** Munitions controls and EPCI authorities are central to being able to regulate export transactions of real concern. The core of EPCI is the U.S. ability to stop particular transactions and to identify particular entities as being of concern. This core must be
strengthened through greater information sharing. The United States needs to expand both its entities lists to better reflect proliferation activities and also needs to greatly expand government efforts to provide companies with information about suspect transactions. It also needs to ensure that companies properly target their EPCI efforts by focusing screening on a positive list of items rather than on a broad range of commodities. If serious about EPCI, the United States needs to consider using information technologies, intranets, dedicated Web sites, and automated screening processes to share information about projects of concern with computer companies.

- The Department of Defense must establish a process to identify and protect military-specific software and databases, using both software protection technologies and munitions export controls.

- Congress should review existing and proposed legislation to strengthen the information-sharing process that is central to nonproliferation controls.

- The National Security Council and the Departments of Commerce, Defense, and State should develop and implement programs to review and strengthen existing EPCI controls and expand the flow of information to exporters by
  -- Expanding the Entity List;
  -- Developing additional outreach programs through presentations, work with Industry and Exporter Associations, and the use of Web-based technologies;
  -- Reforming the “is informed” process to increase the number of potential exporters informed about end-users of proliferation concern;
  -- Focusing screening on items and countries involved in proliferation by developing a positive list of items for EPCI screening and by identifying the dozen or so countries involved in proliferating weapons of mass destruction (WMD) as targets for WMD screening.

Build Military Superiority. To maintain U.S. military strength, the United States needs to take advantage of its preeminence in most information technologies to move forward in three areas. It should partner more closely with information technology companies and universities; obtain and integrate innovations and change doctrine and practices accordingly; and build a strong foundation of education and research to ensure that U.S. technology is as advanced in 10 years as it is today. To do this, the United States will need to consciously strive to be the best systems integrator of the new information technologies—controlling the integration knowledge and continually investing in “leap ahead” technology to maintain a qualitative edge. Partnership with the private sector and universities is central to running faster. The government needs new vehicles for this partnership, perhaps using a range of new advisory committees, exchange programs, and joint projects to provide the latest innovations to DOD. Success will require finding ways to streamline the acquisitions process to bring those innovations more rapidly to government service.
• The Department of Defense should establish new vehicles for partnership with the private sector, including Federal Advisory Committee Act (FACA) committees, industry detaillee programs, and joint innovation centers.

• The Department of Defense, with its congressional oversight committees, should identify and change those acquisitions rules that prevent better use, or refreshment, of information technologies.

• As part of these changes to acquisitions regulations, DOD should establish a task force to begin a fast-track program to adopt an automated supply chain portal similar to that used in the automotive and aviation industries, among others.

• The Department of Defense should identify, develop, and fund five “quick start” programs to incorporate private sector information technology innovations into national security applications.

• DOD, the White House Office of Science and Technology Policy, the NSC, and other relevant agencies should develop broad legislative proposals to expand education programs for information technology and create long-term programs for funding long-range research and development program for information technologies.

• DOD and Congress should consider using a scholarship model where the United States would pay for higher education in computer sciences in exchange for a commitment to service for a number of years.

• DOD and the NSC should identify and implement measures that expand current efforts to reduce vulnerabilities to the Defense Department and to critical infrastructure resulting from increased use of information technologies.

• The intelligence community should develop and expand programs involving private sector expertise to assess what other nation’s forces and intentions are for information technology.

Agreeing that MTOPS-based controls no longer work is easy. Deciding on what policy should replace them is hard, given the political symbolism of computers and the uncertain post–Cold War security environment. These recommendations, in combination, will do more than any other measures relating to information technology controls to give the United States the tools it needs to maintain its military strength.
Chapter 1

A New Context for Controls

“Globalization is not a policy option but a fact to which policymakers must adapt.”

Computer Exports and National Security in a Global Era

In the movie 2001: A Space Odyssey, HAL 2000, the computer with a chillingly calm voice, took control of a spacecraft away from its crew. The film made powerful computers a symbol for the products of twentieth-century science, which at times appears to be escaping the control of its creators. This symbolism has helped shape the debate over export controls on computers and microprocessors by giving computing hardware an undeserved mystique. In 1998 Congress decided that the Clinton administration had done too little to prevent the export of supercomputers to hostile countries. Congress enacted legislation that defined a supercomputer and established difficult procedures for their export. However, important changes in technology and the international environment call into question the current U.S. approach to export controls. These changes are the expansion in performance capabilities and access to computing power; the development of a global market and manufacturing base for information technology; and the decline of multilateral cooperation on nonproliferation and security. To help policymakers determine how to advance U.S. interests in this new environment, this report looks at key aspects of this complex problem:

-- the global context for trade, security, and the rapid pace of technological change;

-- the computing requirements for military and proliferation purposes, including the proliferation of nuclear weapons;

-- the status of multilateral controls on information technology; and

-- the implications of increased access to computing power and networks for U.S. security.

After World War II, the United States developed a strategy that had two equally important but somewhat contradictory objectives. On the one hand, the United States sought to create a stable political and economic international order based on international trade and investment. On the other hand, it sought to contain the Soviet Union by denying communist countries access to the most sensitive Western technology and products. This strategy was successful. Now the United States is left with the policy residue of that era.

U.S. security and foreign policy is still adjusting to the end of the Cold War. Understanding the changes that resulted from the end of this conflict is crucial for assessing current policies and shaping new ones. The United States engaged in a strategy of technology denial
The collapse of the Soviet Union removed the single largest obstacle to economic integration and trade. Travel, communication, and cooperation between the two sides of this conflict were restricted. Limited communications, allied cooperation, and the very real Soviet threat made broad export restrictions on advanced commercial technologies sensible and effective.

The collapse of the Soviet Union removed the largest obstacle to economic integration and trade. The World Trade Organization reports that international trade has increased from $1.8 trillion in 1983 to $5.5 trillion since the Cold War. Long-standing U.S. policies have accelerated the emergence of a more integrated world economy since the Cold War. After World War II, the United States and its allies built international institutions that would promote international stability by removing the barriers to international economic activity that many saw as the root of the Great Depression and World War II. U.S. foreign policy goals included economic stability, free trade, the rule of law, and stable great-power relations. Success has been gradual and incomplete, but these policies have produced stabilizing and integrative effects in the global economy.

Technological change has reinforced economic integration. Improved telecommunications and the creation of the Internet allow rapid, cheap, and accurate transfers of information. Improvements in transportation have been equally important. Container ships have led to dramatic reductions in bulk transport costs. Jet engines and the very large transport aircraft they power revolutionized international travel and, more recently, the transportation of goods by air. Air transport is now cheap enough that cargo aircraft routinely transport high value or specialized goods—computers, aircraft parts, satellites, and even automotive air bags. In combination, these changes in telecommunications, air travel, and shipping have created unprecedented mobility of goods, people, and ideas.

One result of this is greater international commercial and technical collaboration. A series of annual studies by the National Academy of Science has found that research has become more international and more collaborative. Scientific research has become more international as more countries have developed scientific capabilities and as scientists see the benefits of research conducted by multinational teams of specialists. International research and development alliances among corporations have increased eight-fold since the mid-1980s. Companies place plants and development centers in different countries to ensure market access and to move ideas quickly among these facilities to gain competitive advantage in manufacturing and research and development in a global marketplace.

This sweeping international economic integration is called globalization.
Reducing the obstacles to, and costs of, international trade mean that industries are increasingly integrated along lines of lowest cost rather than national borders, based on the free play of comparative advantage, economies of scale, and innovation. Specialization means the lowest-cost producer may be another country, and subcontracting has become increasingly international. Competitors are no longer geographic neighbors, and suppliers may be located a continent away.

Broad military and security trends reinforce economic globalization. The end of the Cold War was the end of a long cycle of conflict among industrialized countries that began in the nineteenth century. The risk of war among the developed states is as low as it has ever been, creating a security and political climate conducive to economic integration.

However, the emergence of powerful new states and increasingly problematic non-state actors means that the United States will face new challenges in the post–Cold War security environment. Among the key changes: China and India are entering the ranks of the great powers. The United States has gone from leading an alliance of Western industrial democracies in a global defense against a mirror-image superpower to a world where alliances are less cohesive and threats more diffuse. Terrorism and relatively crude weapons of mass destruction pose a greater threat to the United States than conventional military conflict. Regional conflicts in the Middle East, Asia, and Africa threaten international stability and U.S. interests, especially when the proliferation of weapons of mass destruction is thrown into the mix. The United States now faces a different and more complex security environment that continues to evolve. This complex pattern of relationships challenges U.S. foreign policy and the U.S. export control system in ways unforeseen a decade ago.

Sell Globally or Go Bankrupt Locally

Integration and globalization have changed how companies must operate if they are to remain financially and technologically viable. Expanded international trade means that specialization of production can occur across borders and that companies will be more competitive if they use foreign suppliers or invest in foreign subsidiaries. Firms “specialize” in activities in which they have a competitive advantage. Companies can now buy from the lowest-cost supplier whether they are located in a different country or even a different continent. If they do not buy from the lowest-cost supplier, if they ignore the global market, they will lose money and market share. These forces shape the information technology industry.

Manufacturing has become a global activity because it has become much easier for companies to take advantage of production cost differentials.
In the high-tech economy, ownership of intellectual property can be more valuable than control of manufacturing plants. Between countries. Reductions in transaction and transportation costs allow producers to spread design and manufacturing around the world to take advantage of lower costs. The result is a process where it is normal to manufacture components in several countries and assemble them in another, none of which may be the home country of the company whose label goes on the shipping box. Subcontracting of manufacturing and assembly is the norm—companies like Flextronics or Solectron specialize in assembling other firms’ products on a contract basis. In the high-technology economy, ownership of intellectual property is increasingly more important and valuable than control of manufacturing capabilities.

With manufacturing widely dispersed and with the strong international demand for information technology, firms in many countries have entered the market as suppliers.

Table 1.1. Foreign IT Assembly: Manufacturing and Research Capabilities

<table>
<thead>
<tr>
<th>Country</th>
<th>Semiconductors</th>
<th>Computers</th>
<th>Components</th>
<th>Software</th>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td></td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td>F</td>
<td></td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>F</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td></td>
<td></td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>France</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>F</td>
<td></td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>F</td>
<td>F</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td>F</td>
<td>F</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td></td>
<td>I</td>
<td></td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Japan</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Korea</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td>F</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Philippines</td>
<td>F</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td>F</td>
<td></td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>F</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td>UK</td>
<td>F</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

Note: I—Indigenous capability; F—capability from foreign subsidiary.
Source: U.S. Department of Commerce; Merrill Lynch; Gartner Group.

Relatively low barriers to entry by new suppliers for some information technology sectors (software, component assembly) help make the market more competitive for the United States. The United States does not have a monopoly on information technology. Foreign substitutes are available for U.S. products.
very competitive. Foreign firms enter the market in these areas and then try to expand. The Chinese company Legend, for example, began by assembling single-chip desktop models and now manufactures multiprocessor servers.

The United States leads in market share for many sectors, but this fact is due more to U.S. firms’ successful business strategies than to any monopoly on technology. Foreign producers are increasingly available as substitutes for U.S. producers, for both microprocessors and computers. The leading microprocessor firms include Intel, Sun, Advanced Micro Devices, IBM, Hitachi, Fujitsu, Siemens, Phillips, and STS Microelectronics (formerly SGS Thompson). An even larger number of firms (in Taiwan, Korea, and Japan) compete in the memory chip market. U.S. firms currently dominate the logic chip market, but to constrain U.S. producers from participating in the global market would create a market space that foreign firms would successfully exploit.⁴

In previous technology “revolutions” (steam engines, internal combustion, electricity, and telephones), access to new technologies and the ability to produce them originated in a few advanced countries and then spread to others. The same pattern applies to information technology, except that the rate of diffusion is faster. U.S. firms have a technological and market lead that discourages some foreign competitors from entering the market, but others in Europe and Asia are eager to share in the revenue stream.

Performance and Technological Improvement

“Everything having to do with digital technologies gets relentlessly faster, smaller and cheaper.”
—Larry Downes and Chunka Mui, *Unleashing the Killer App* ⁵

The global market rewards companies that introduce leading-edge products with greater market share. Companies that continue to use older technologies lose money. This economic force has driven the rapid increase in computer and microprocessor capabilities. Computers have advanced in many directions, but notably in the ability to process increasingly large volumes of data at ever faster speeds. During the past decade, this phenomenon was expressed by a single measure that ultimately Congress wrote into law—MTOPS, or “millions of theoretical operations per second”—to represent a computer’s estimated “power.” The problem is that the supercomputer of 1990—a computer then manufactured only in the dozens of units—had by the year 2000 become the laptop manufactured in the hundreds of thousands.

Improvements in microprocessor performance are the key to understanding the increase in access to computing power. Microprocessors are integrated circuits built on a small square of silicon. Each contains superfine metal lines that interconnect millions of transistors. The transistors work together and
enable the microprocessor to perform a variety of functions. Mass-produced commercial microprocessors known as CPUs (central processing units) are the brains of modern computers. The low-cost, mass-produced microprocessors that first enabled the creation of cheap, portable, single-chip personal computers can now be combined to form increasingly powerful systems.

In 1965, Gordon Moore of Intel, a leading U.S. chip manufacturer, realized that each new generation of chips had roughly twice as much capacity as its predecessor, and each generation appeared within 18 to 24 months of the previous chip. This meant that computing power would expand exponentially over short periods and at significantly lower costs. His finding, now known as Moore's Law, has proven to be surprisingly accurate.

Figure 1.1 shows the increase in the performance of widely available CPU microprocessors. These commodity chips form the basis of commercial computers. The most powerful mass-market chip available in the beginning of the 1990s operated at roughly 4.5 MTOPS. Today the most powerful mass-market chip available operates at 4000 MTOPS, and faster chips will be available in the next year.

The key to dramatic increases in microprocessor performance lies in improvements to the manufacturing process and, in particular, improvements in photolithography. Photolithography is the manufacturing process that transfers circuit patterns onto semiconductors. The smaller the size of the pattern being projected onto the microprocessor (known as “feature size”), the more circuits can be crammed onto a microprocessor and the higher its speed (known as “clock rate”), increasing its performance. Feature size is measured in microns. A micron is one-thousandth of a millimeter (a human hair is 100 microns thick). Over the past 30 years, lithography manufacturers have been able to reduce line widths from 10 microns in 1971 to 0.18 microns in 2000.
Figure 1.2 shows the decline in feature size—not surprisingly it is the inverse of the increase in microprocessor performance. State-of-the-art equipment now produces a line width of 0.11 to 0.13 microns.

A similar trend can be observed with supercomputers. Twenty years ago, a “supercomputer” operated in the range of a few hundred MTOPS. Today, the most powerful computers operate in the millions of MTOPS. Figure 1.3 shows the most powerful computers on the Top500 Supercomputer Sites’ annual lists of the world’s most powerful computers, using GFLOPS (1 billion floating point operations per second), a common measure of performance used in the scientific community.

The Reagan administration’s decision in the 1980s to release microprocessors and low-level computers for export to the global market proved to be of immense economic advantage to the United States. Microprocessors, computers, and the information technology they enable have been the engine of growth for the United States in the past decade. However, this decision also led to the emergence of mass production and the creation of a global market for information technology hardware. The result is that computing power, relatively scarce a decade ago, is now abundant.
Access to Computing Power

“Today’s high-end systems are no longer designed with the scientific user in mind. Instead, the key building block is a microprocessor that most likely has been designed to run Excel or some other tool from a suite such as Windows.”
—National Science Foundation

Ten years ago, extremely large amounts of computing power required an extremely large computer. Not so today. There are now many ways to obtain access to high performance computing power without a high performance computer—including, for example, assembling a high performance computer using mass-market microprocessors; “clustering” mass-market microprocessors or desktop computers; and using the Internet to link computers in numerous locations to achieve high performance. Because CoCom did not foresee these methods when it created computer export controls, they are not subject to export controls, and any effort to control them would be ineffective, given the relative simplicity of the technology and the widespread availability of the basic hardware.

Traditional supercomputers were “vector” systems using specialized components. Vector machines were easy to control. They were expensive and scarce—specially built machines using specially designed microprocessors and requiring special code for their use. The development of parallel processing as a competitor to the vector machines allowed mass-market components and networks of basic computers to perform as well as traditional supercomputers. Parallel processing is a programming technique where tasks are broken into smaller parts, each of which can be attacked simultaneously by a number of processors. Researchers developed alternate methods of programming to use massive arrays of general-purpose microprocessors as a lower-cost alternative.
In recent years, parallel processing machines have overtaken traditional supercomputers in performance. The ability to break down problems into discrete bits means that general-purpose microprocessors, whether assembled in one machine or in a group of networked machines, can solve most of the problems that once required a supercomputer. The lesson is that software, which requires no special equipment to write, could substitute for the specially built (and easily controlled) supercomputer hardware. Vector machines may still have an advantage for solving certain problems, but some experts believe even this advantage will disappear within two or three years.  

Many companies, universities, and research institutions around the world now have the ability to assemble a powerful computer from commercial components and software not controlled for export. Commodity-level microprocessors of the kind used in desktop computers can be clustered to provide high performance computing (known as “commodity clustered computing”) using low-level commercial “interconnect” technologies. Clustered supercomputers have their own “Top 500” Web site (http://clusters.top500.org). The most powerful clusters are capable of performances in the hundreds of GFLOPS, which are equal to hundreds of thousands of MTOPS (billions of floating point operations, a standard measurement of a computer’s speed in performing mathematical operations).

Some assert that commodity clusters cannot go above 80,000 MTOPS. However, many foreign clusters are more powerful. A cluster of 528 Pentium III processors at Chemnitz University of Technology in Germany performs at 422 GFLOPS equal to 392,000 MTOPS. Microprocessor clusters can be easily expanded without outside help. The General Accounting Office concluded that “the current export control system for high performance computers . . . is ineffective because it cannot prevent countries of concern from linking or clustering many lower performance uncontrolled computers…”

Retail computers can also be connected to form a single system to provide powerful and increasingly sophisticated computational resources, using commercial interconnect hardware and widely available software. The ability to link desktop computers allows potential proliferators to draw on a population in the hundreds of millions for their needs—one report estimates
there are more than 384 million computers worldwide, with an additional 130 million desktops sold in 2000. This large installed base of computers outside the United States makes high performance computing for many applications a problem that depends more on finding the right software than on gaining access to hardware.

Network improvements also increase access to computing power. In the next few years, network improvements will join increased microprocessor performance in driving computer performance. A few companies are now using the Internet to combine thousands of desktop computers in a numerous locations into a single computing system. The next generation Internet, with its greater “bandwidth” (a measure of the amount of information that can be passed over a network) will provide even greater access to high performance computing. Researchers have begun to refer to a computer “grid” that will, like the electrical power grid, provide researchers with broad access to high performance computing using autonomous programs that can move themselves without human help among computing centers in different countries to take advantage of available resources.

All of these substitutes provide equivalent performance to supercomputers and make computing power widely accessible. Substitution is central to understanding the control environment for computers. Microprocessors, linked desktop computers, and network computing are all viable substitutes for high performance computers. Denying access to high performance computers would shift demand to one of these alternatives—as now occurs when poorer universities substitute cheap clusters for more expensive systems.

How these substitutes affect microprocessor and computer export controls can now be predicted. Export controls restrict trade and, if they work, create a targeted scarcity in computers by reducing the supply (because the government does not permit certain exports to occur). The initial effect is that the price of computers will increase in response to unmet demands from buyers. The second effect will be for new suppliers and alternative products to appear in response to meet that demand. The greater the demand, the faster alternative sources of supply will appear. Export controls can remain effective only if they capture these alternative manufacturers and substitute goods.

If there are few other suppliers and few substitutes for computers, export controls will raise their price. This could have the positive effect of making a program of concern more expensive for proliferators. However, if there were many suppliers or many substitutes, sellers could not charge a higher price for computers, thus incurring no additional cost to a program of concern.
The availability of alternative products and suppliers makes the supply of computing power more “elastic,” an economic term referring to the market’s quick ability to find alternative supplies in the face of shortages. When supply is elastic, as it is with computing power (given the broad range of substitutes), it affects U.S. export restrictions by shifting demand from U.S.-made products to other sources of computing power.

The Central Intelligence Agency’s annual report to Congress on proliferation provides evidence of substitution and elasticity in foreign WMD programs. It notes “Countries determined to maintain WMD and missile programs over the long term have been placing significant emphasis on insulating their programs against interdiction and disruption, as well as trying to reduce their dependence on imports by developing indigenous production capabilities. Although these capabilities may not always be a good substitute for foreign imports—particularly for more advanced technologies—in many cases they may prove to be adequate.”

Recent press reports note that the Defense Intelligence Agency was concerned that Iraq had built a supercomputer using 4,000 units of PlayStation 2 provide another example. The PlayStation 2 uses a powerful processor that, if Iraq could overcome software and networking problems, could combine to reach teraflop-level performance. Although it is possible to combine the PlayStations, if Iraq wanted powerful computing it would be easier to use off-the-shelf network hardware to connect the low-level PCs it has been able to acquire. The juxtaposition of PlayStations and nuclear proliferation may appear ludicrous, but it only demonstrates the growing ubiquity of high performance computing in everyday applications.

These developments have serious implications for current U.S. export controls. Computers and microprocessors are commodities that can be purchased around the world. Computing power is no longer scarce. Even the most draconian measures cannot prevent “leakage” of computers sufficient for military purposes. Even Iraq, under the tightest embargo possible today, has been able to obtain commodity-level computers. In its own investigations, the Department of Defense concluded that current controls “do not restrict foreign access to high performance computing.”

**Conclusion**

National security can be defined at two levels. Narrowly it depends on the quality of U.S. weapons and the readiness of U.S. forces. This focused definition of national security historically included restrictions on exports as a way of holding back the technical progress of U.S. opponents.

National security also can be defined as the vitality and strength of the U.S.
economy and the dynamism of American society. The United States won the Cold War not because it fielded a stronger military than its opponents, but because American societal values and the dynamic U.S. economy proved to be an overwhelmingly superior model for the future.

The development of computers and information technology was crucial to both dimensions of national security. Computers and information technology fueled the “revolution in military affairs” that transformed the U.S. armed forces into the mightiest military establishment in history. Blocking access to that technology during the Cold War constituted an important dimension of U.S. strategy.

Computers and information technology also represented the creative wellspring of the explosion of U.S. economic strength and productivity. The U.S. economy dominates the world today in no small measure because of the microprocessor and the business models created around the revolution in information technology. Like an iceberg, U.S. military might is just the 10 percent that rises above the waterline. The 90 percent base of U.S. national security rests on an economy and society that have grown thanks to this industry.

Export controls must now be fundamentally reassessed. They no longer constrain the activities of other nations because supercomputing is no longer limited to supercomputers. Moreover, they are starting to impinge on the vitality of the U.S. economy, potentially eroding an industry that America needs for its long-term vitality.
Chapter 2

Proliferation and Cooperation

“One 486 chip has more computing power than U.S. scientists had when they developed the first atomic bomb.”

—Philip Heerman, computer scientist, Sandia National Labs, Quoted in Wired Magazine, April 2001

Critics of control threshold increases believe that high performance computers are sensitive “enabling” technologies for nuclear weapons, missiles, submarines, and other military applications. It seems reasonable to assume that if computers and microprocessors are the engines of economic growth, they are also engines of military strength. Such a premise, although certainly true in the 1970s and probably true in the 1980s, is no longer valid today. The dramatic increase in computing power over the past 10 years and the transformation of computers from highly specialized research tools in the 1980s into a mass-market infrastructure in the late 1990s breaks the connection between high performance computing and weapons proliferation.

Fundamentally, military applications do not require much computing power. This is especially true for design and manufacturing. The United States designed and built its weapons and military equipment with computers of 500 to 1000 MTOPS. At the time, these were large, sophisticated supercomputers, and high performance computers as they are known today did not exist. The same computing power or more is now available from a good desktop computer or workstation now commonly found in offices and classrooms.

For example, the F-22, the most advanced U.S. fighter, was designed with a 958 MTOPS Cray supercomputer, roughly one-quarter the power now found in mass-produced Pentium chips. High performance computers are not necessary for foreign military or nuclear weapons programs and foreign weapons do not depend on access to computing power. Computing power is considerably less important than the ability to integrate materials, manufacturing equipment, and skills into a modern weapon. This ability to integrate disparate technologies requires years of experience in design, operation, and manufacturing. Faster computers can cut program run times, but the output is the same, and saving a few hours in programs whose lengths are measured in years does not provide an advantage.

Despite frequent charges that computers make a substantial contribution to foreign weapons of mass destruction (WMD) programs, these programs also do not require high performance computers for their design and construction.
The most telling example of this is that after more than a decade of review, none of the multilateral WMD nonproliferation regimes control computers—the Nuclear Suppliers Group, the Missile Technology Regime, and the Australia Group. These regimes, led by the United States, have concluded that computers are not especially significant for proliferation, given the very low levels of computing power needed for design and manufacturing.

This is particularly true for nuclear weapons. The U.S., Soviet, British, French, and Chinese nuclear arsenals were designed without high performance computers. First generation weapons were designed and produced entirely without benefit of computers. One proliferation expert notes:

At one time computers, useful for numerical simulation in weapon design, were considered a restricted technology that limited the ability of other nations to develop weapons. However, this capability is most important for thermonuclear weapon design, not fission weapons. The computational effort required for the neutronic and hydrodynamic computations used in fission weapons is actually quite modest, easily within the capability of any commercial PC available today. Even with thermonuclear weapon design, computational requirements are not that extreme. The design efforts for most weapons in the US arsenal were completed well before the microprocessor revolution of the 1990s. A high-end workstation is comparable or superior to the best computers available when most current US warheads were developed. Even the lowest performance office computers now on the market are orders of magnitude faster than the computers used to design the first hydrogen bombs. 24

Numerous studies have reached this conclusion. Studies by Etter, Goodman, and others note that computing power is less important than access to test data and specialized software. Sophisticated simulation capabilities can permit nuclear weapon states to reduce or even eliminate the need for weapons tests to develop or prove a design. However, computational power is of little benefit unless the computer is running sophisticated codes based on extensive experience and data—in particular, data derived from actual nuclear weapons explosions. A country without extensive experience in weapons design is at a significant disadvantage, and the lack of reliable data and proven codes will substantially constrain the usefulness of computer technology. 25

First or second generation nuclear weapons of the kind proliferators are attempting to manufacture need very little computing power for their design...
or manufacture. Designing the next generation of nuclear weapons needs immense computing power—power of a kind that now can be obtained only from machines capable of millions of MTOps. Only a few U.S. laboratories and agencies have these large, expensive, specially designed machines.

Computers can contribute to military capabilities in ways other than the design and manufacture of weapons. Examples of such applications are shown in figure 2.1. A key objective of the Cold War export control system was to prevent the Soviet Union from obtaining Western microprocessors and computers for use as components in weapons systems or in military applications such as antisubmarine warfare, air defense, battle management, and weather prediction. This objective lives on in our export controls despite the radical change in the international security and economic environment.

Figure 2.1

Many applications essential to national security require very small amounts of computing power.

Work by Goodman, Wolcott, and Homer provides a range of MTOps used in military applications. Many of these applications can be run using clusters of commodity computers. Cluster computing provides very high performance for most military applications, but it is not suitable for mobile battlefield applications. However, the need for high performance computers in battle management applications is overstated. Many military applications use mass-market desktop computers, workstations, and servers. In many cases, high performance computing is used to develop the necessary software codes for battle management, not to run them. Data collected by platforms such as aircraft or submarines are taken back for analysis and processing. Clustered computers can be used in this processing phase to analyze the collected data and produce software applications and codes to be sent back to aircraft and
ships for battle management and combat purposes. These codes can then be run on less powerful machines.

The United States itself used elderly 650 MTOPS VAX computers until recently in the J-STARS battlefield surveillance aircraft. Although computers of this level are now widely available, the VAX is no longer produced. The computers used on the EP-3E Aries II (the aircraft involved in the recent incident with China) uses 1997 workstations capable of 240 MTOPS. Both the JSTARS and the EP-3E used computers that are at least a generation or two behind what is available on the retail market. In addition, few countries can afford to attempt to mirror U.S. battle management systems—they are more interested in finding where these systems are vulnerable.

Computing power is important in performing these functions, but less critical than the ability to integrate computers, sensors, and platforms into effective systems that can operate on the battlefield. The crucial element for many of these applications is the sensor. For the foreseeable future, the United States faces no likely competitors in fielding advanced space-based and aircraft sensors. This limits the utility of access to computer power for any potential opponent to that information that can be obtained from commercially available imagery and from traditional sensors, such as ground-based radars and aerial photoreconnaissance.

One national security function—cryptanalysis—deserves separate discussion. Specially modified computers with very high performance remain useful for cryptanalysis, but clustered low-level computers can provide this level of performance. The National Security Agency (NSA) also uses very powerful, specially designed microprocessors and computers for cryptanalytic purposes, but these are not general-purpose items sold on the commercial market. They would be controlled as munitions for export purposes. NSA became indifferent to export controls for commercial high performance computers several years ago.

An energetic political debate has exaggerated the role of computers in military applications. Assembling conventional weapons or weapons of mass destruction, requires a package of skills, equipment, and technologies. The ability to integrate these various elements into a modern weapon requires deep experience in design, operation, and manufacturing. It may require specialized databases and, in many cases, test data assembled over a period of years. These elements are more important than the speed at which the data are processed. Computers are only a small part of the skills and equipment needed to build weapons. More important, high performance computers can be replaced in a weapons program by an average desktop or workstation and a strong national software capability.

---

**JSTARS: 650 MTOPS**

**EP-3E: 240 MTOPS**

**Apple Laptop: 2018 MTOPS**

Technological improvements have eroded the proliferation and security rationale for controlling commercially available hardware.
Conclusion

The popular image of computers suggests that they are essential to arms production and proliferation. This notion is intuitively appealing—given the role computers play in the economy, in research, and in U.S. weapons development programs—but misleading. Information technology is crucial to military applications, but computer speed is not. Performance increases in basic microprocessors and desktop computer sold in the millions, combined with software and applications developments, mean that today’s low-level systems provide all the computing power needed for military and proliferation-related applications. Technological improvements have eroded the proliferation and security rationale for the control of commercially available hardware. Military advantage results from specialized software and applications more than the power of the computers available. One result of these changes has been a marked reduction in support among U.S. allies for continued controls on information technology.
Chapter 3

Multilateral Cooperation on Export Controls

“The current unilateral system is the worst of all possible worlds. When the U.S. denies permission…to sell abroad, and our allies step in and make the same sale, our national security isn’t protected—and our nation’s competitive position is harmed.”
—Congressman Christopher Cox

During the Cold War, the United States led the Western world in establishing a systematic process to keep advanced technology out of the hands of the Soviet Union and its allies. Actually two separate systems emerged. One was a comprehensive arrangement to keep military equipment and militarily relevant commercial equipment out of the hands of the Soviet Union. During the 1980s and 1990s, a parallel arrangement developed to prevent the proliferation of knowledge, equipment, and relevant materials that could be used to build unusually dangerous weapons-chemical, nuclear, and biological weapons, and long-range missiles to deliver them. This second system was designed to limit the proliferation of these technologies and equipment from leaking to a much larger set of countries.

Four regimes—the Nuclear Suppliers Group, the Missile Technology Control Regime, the Australia Group, and the Wassenaar Arrangement—provide the multilateral framework for export controls. The latter organization controls the export of information technology. Wassenaar also differs from the others in that it focuses on general-purpose industrial equipment and conventional arms rather than on weapons of mass destruction.

The nonproliferation regimes have broad and sustained multilateral support and have worked hard to establish an international norm that supplying missile or rocket technology for military purposes is unacceptable behavior for states. The multilateral regimes for missiles, nuclear, chemical, or biological weapons are effective in making it more difficult for proliferators to acquire key technologies. The regimes have a focus on crucial components and specialized production equipment. There is broad political support from member states for the mission, and the regimes have focused, agreed goals.

The members of these regimes have chosen not to control computers. Computer controls began with CoCom—a Cold War arrangement developed to ensure NATO’s qualitative edge over the Warsaw Pact forces’ numerical advantage in military equipment. The United States created computer controls in the days of large, expensive mainframes that were difficult to transport and whose primary use was for research. CoCom controls predate the rapid,
continuous expansion of computing power that began in the 1990s.

CoCom’s successor, the Wassenaar Arrangement, retained computer controls. This regime is by any measure a different kind of regime than its nonproliferation counterparts. Unlike CoCom, there is no agreed threat for Wassenaar members. Unlike the nonproliferation regimes, most of the items controlled by Wassenaar are widely traded and a part of normal commerce. Disputes between the United States and its partners are frequent, reflecting wide disparities in foreign policies. Many disputes have been over information technology, resulting from the lack of a strategic rationale for continued controls and by the U.S. penchant for amending national controls in advance of consulting its partners.

Wassenaar controls four categories of information technology: telecommunications, encryption, microprocessors, and computers. CoCom controlled these same categories. The trend in Wassenaar is to decontrol these technologies. Over the past five years, most information technologies other than computers and microprocessors—software, telecommunication switches, fiber-optics, software—have been released from multilateral control and are now exported freely to all destinations (except Iraq) by European, Japanese, and non-Western manufacturers. Wassenaar member states argue that although control had been an appropriate part of economic warfare against the Soviet bloc, information technology is now a routine part of normal civil commerce and control is no longer justified.

Wassenaar began by decontrolling telecommunications equipment in 1995, including the switches and fiber-optic technologies that form the backbone of large computer networks, in the face of intense pressure from Germany with support from France and Japan and despite vigorous opposition by the United States. In 1998, Wassenaar members pushed for the decontrol of encryption software because it was widely available and essential for electronic commerce. The United States originally blocked decontrol, but found that although it could prevent Wassenaar from taking encryption software off the multilateral control list, it could not prevent countries from exporting most encryption products under some form of automatic approval to all destinations. In 1999 and again in 2000, the United States acceded to partial decontrols for encryption.

Wassenaar members argue that there is no longer a strategic rationale for computer and microprocessor controls. The Netherlands, Germany, and the United Kingdom have been leading advocates of decontrol. Wassenaar rejects the argument that controls on microprocessors and computers are needed to ensure that they do not go to “pariahs” like Iran—members argue that this is a U.S. effort to force them to cooperate with the U.S. unilateral embargo on terrorist nations. The debate in Wassenaar has turned from controls on
hardware and end-items (despite U.S. objections) to the question of whether and how to control production equipment for information technologies (such as photolithography) and the technical expertise to build these products.\textsuperscript{35}

Similar problems have dogged the bilateral supercomputer regime the United States created with Japan. In the 1980s, the United States decided to supplement CoCom with a bilateral arrangement with Japan to control supercomputers. This arrangement made sense, as Japan and the United States had the largest computer industries and built the most powerful computers. The bilateral arrangement involved a prior consultation process where each country would notify the other before approving the export of a supercomputer and an agreed set of conditions and safeguards that would be applied to exports.\textsuperscript{36}

Over time, poor coordination and the lack of a strategic rationale have eroded the bilateral regime. First, as the U.S. share of the high performance market increased disproportionately, almost all of the prior consultation consisted of America’s notifying Japan of its licenses. In the past five years, Japan has not submitted any licenses for review, according to the Department of Commerce, and has never objected to a proposed U.S. export. Second, U.S. intransigence in Wassenaar over reforming control on information technology irritated the Japanese, who suspected that the United States must have a commercial motive rather than any military or nonproliferation goal. Finally, Japan was increasingly frustrated by the U.S. habit of failing to consult in advance of changes to its national computer controls, despite a clause in the bilateral agreement that required such advance consultation.

Japan has asked to terminate the bilateral supercomputer agreement, as it no longer has any strategic relevance. Given the limited utility of the bilateral regime, agreeing to end it only requires structuring the termination in a way that does not damage other areas of Japan’s export control authorities. This may require keeping some arrangement where Japan would agree to continue to control computer exports to countries like Iran, Libya, and North Korea.

In the current climate of very limited multilateral cooperation, the United States would be hard-pressed to keep information technology out of the hands of potential opponents even if computing power had not become ubiquitous. Could we rebuild cooperation? Absent a common strategic rationale, this would be difficult. The Europeans are loath to support the embargo of Iran and have explicitly rejected a new embargo on China. The United States would also face difficulties in persuading others to recontrol commodity-level items (such as microprocessors, workstations, and servers) when the strategic and nonproliferation rationale for such controls has been widely discredited.
The Question of MTOPS

“MTOPS is an outdated measure….”
—General Accounting Office

The core of CoCom-based controls is MTOPS—a measure of computer performance created in the early 1990s. The term is not used by industry or science, but was developed solely for export control purposes. The MTOPS system has come under some pressure as the government has been forced over the past decade to make drastic increases in control levels to avoid having to license millions of commodity-level computers. The rapid advance of microprocessor and computer technology means that system performance increases faster than export controls can follow.

MTOPS are increasingly useless as a measure of performance. The MTOPS metric does not accurately reflect the performance of the information technology on the market today. Microprocessors of similar performance capabilities can have vastly different MTOPS ratings. MTOPS is a static measure that does not work for measuring the performance of networks or clustered systems, which can increase rapidly as new chips or computers are added. Government and industry have explored several alternatives to MTOPS—none have been satisfactory. Appendix A briefly reviews some of the alternatives.

No replacement has proved satisfactory because MTOPS serves a system that is no longer congruent with technology. MTOPS or any other benchmark needs to be continuously updated as microprocessors and computers improve. More important, all hardware performance benchmarks fail to measure computing power derived from networked computers. Benchmarks made sense when a single, stand-alone box was the source of computing power. They are increasingly irrelevant in a world of computer networks where the network performance is dynamic—increasing as improved software or uncontrolled hardware is added. Neither MTOPS nor any other parameter constitutes an inadequate measure of system performance. The best alternative may be to simply eliminate MTOPS, and with it, the dual-use controls inherited from CoCom.

Proposing to eliminate MTOPS-based hardware controls could give the US some much needed credit in Wassenaar.

The MTOPS metric was created as an element of a multilateral dual-use control system, and its end should also be multilateral. The United States can gain some credit by proposing in Wassenaar to end MTOPS-based hardware controls. With a new administration in office, the United States has an opportunity in Wassenaar to repair some of the damage of the past five years. It may wish to include with the proposal to eliminate controls on computers the idea of a broader reexamination of the remaining information technologies controlled by Wassenaar. Such a proposal could fit into a larger (and necessary) reexamination of the regime and its purposes. An adroit
handling of the U.S. proposal in Wassenaar could provide the United States with a quid (albeit a small one) to trade for support for other initiatives.

It is possible, given the history of negotiations in Wassenaar, that if the United States proposed the elimination of MTOPS-based controls, one or more nations (such as Russia) would move to block any change solely to damage U.S. interests. The United States must take the necessary steps to prepare other nations for a change in policy and be prepared to escalate the matter to senior-level attention at the Wassenaar Plenary to counter any mischievous action.

**The Effect on U.S. National Security**

“The things which give military forces their fighting capability are changing, and these changes point toward a qualitative jump in our ability to use military force effectively.”


The widespread availability of computing power is part of a larger trend identified by the Defense Science Board Task Force on Globalization—the global diffusion of technology. This trend could degrade U.S. national security unless the United States takes effective in response.

Many potential adversaries realize that this trend toward greater access to technology can provide them with advantages and that information technology can be used as a weapon against the United States, though they also fear that a global information network will erode their political control. Their military goals are not to achieve strategic parity with the United States (although force modernization figures highly with all potential opponents), but instead to develop the ability to disrupt or deny the United States its power projection capabilities that allow it to insert a rapid and powerful military presence in their region.

Two developments in particular have shaped this new challenge. First, the experience of the Persian Gulf War made militaries around the world realize that they needed to change. In the conflict with Iraq, the United States used a combination of air- and space-borne sensors, a robust communications network, and precision targeting (through either smart weapons or through ordinary munitions targeted with the Global Positioning System, or GPS). This was not a digital battlefield, but it had many digital elements connected by human interfaces. Iraqi forces found it difficult to compete with an opponent well supplied with space services for navigation, communication, and remote sensing, a superior communications network, and a range of interfaces. Potential opponents around the globe learned from this that they needed to modernize their forces to remain credible and, more important, had to look for new vulnerabilities in U.S. forces created by this high-tech mode
of combat.

The increasing reliance of the U.S. government and economy on computer networks also offers a new and tempting target. Many of these U.S. systems are accessible from the global computer network. The Internet enables instantaneous global communication, but also creates a new potential for access and, with this, new risks. Most computer networks are built with vulnerable technologies designed to allow easy access. This is the legacy of an open, unencrypted network oriented toward easy compatibility and the rapid growth and diffuse technologies that mark the global Internet.

The tools needed to exploit these vulnerabilities are, for the most part, easy to produce, globally available, and cheap. The United States could face greater risk from network vulnerabilities than it does from the potential contribution of high performance computers to weapons production—the traditional concern over information technology exports. Network vulnerabilities are an area of risk that potential opponents are aware of and will attempt to exploit. To defend against these new risks, the United States must look at networks and software applications more than the hardware of high performance computing.

The security implications are profound. First, the United States does not want to become complacent in its use of policies that were effective in the last war. These may not be the best response to new combinations of technology and doctrine that will be used by our opponents in the next war. Second, access to computing power does not translate automatically into military advantage. It is how a nation uses computing power that is important. Information technology will provide an advantage to those forces that are successful at “combining new doctrine and concepts of operation, innovative organizational structures, and more responsive command and control capabilities with advanced weapons systems.” 40

Third, the United States has, for now, an advantage in the use of information technologies. The size and level of development of U.S. forces and its economy provide this advantage by giving the United States greater opportunities to exploit information technologies. No other nation has the range of sensor capabilities, for example, that the United States possesses, and therefore no other nation will gain as much from integrating sensor data into military networks.

Unique U.S. software applications based on years of operational experience and (in some instances, extensive testing) provide a considerable advantage.41 This specially developed software is not available on the commercial market and, despite strong software industries in many other countries, not easy to duplicate without access to specialized data. Much of this U.S. software is
classified and considered a munition for export control purposes. The United States retains unique advantages in military software. A new policy for information technology should focus on this element of the equation, strengthening controls on specialized software and databases and seeking to extend U.S. advantage by developing specialized new software applications.\textsuperscript{42}

Fourth, although policies that attempt to deny access to information technology hardware by potential opponents are no longer effective, there are political and diplomatic benefits to technology denial. These political and diplomatic benefits must be carefully weighed against the potential cost to U.S. economic and technological strength. Export controls have been a useful diplomatic tool in the past, and as part of any restructuring of controls, the United States needs to consider if for these purposes it needs to find alternatives to Cold War export controls.

The United States faces new security challenges because of the unavoidable diffusion of technology. Given the U.S. emphasis and reliance on information technology, potential opponents are exploring how to access to these technologies to exploit potential vulnerabilities. Technology denial, although of benefit for the Cold War and still of benefit for core elements of weapons of mass destruction, is increasingly ineffective for general purpose commercial items sold in global markets. The United States could increase the risks it faces if it relies on attempting to deny access to commercial technology. It must instead emphasize how to minimize its new vulnerabilities and how to take advantage of the new technologies to outperform potential opponents.

\textbf{Post-CoCom Export Controls}

The United States controls exports of information technologies in four ways—first, by controlling computers and information technology specially designed for military use as munitions. Second, computers and information technology are subject to unilateral sanctions and embargoes on countries like Iran or Cuba. Third, the Enhanced Proliferation Control Initiative (EPCI) applies to computers sought for proliferation-related uses. Finally, the United States controls general-purpose computers as dual-use exports, based on its commitments in CoCom and the Wassenaar Arrangement, using a complicated system of MTOPS levels and country tiers. It is this last category of controls that has outlived its usefulness.

U.S. controls on general-purpose computers involve a complex array of license exceptions, MTOPS thresholds, and country tiers. For countries in the first tier (allied and friendly countries), there are essentially no restrictions. For the third tier, which includes countries like Iran and Cuba, restrictions are effectively all-encompassing. For a middle country tier consisting of potential
opponents, proliferators, and countries in unstable regions, the licensing threshold is determined through a process that involves estimating which microprocessors and computer systems are likely to come on the market in six months and what foreigners can produce. The Department of Commerce reports that it receives two licenses a month under this system.

These controls have conflicting tasks: allow U.S. and foreign companies to sell a broad range of computers to a global market while maintaining restrictions on military-related recipients in a small set of countries. Rapid increases in mass-market computing technologies have made this approach increasingly difficult to implement, as has the lack of international cooperation. The Clinton administration streamlined the controls substantially in 1996, 1999, and 2000, but these changes, although beneficial, only postponed the need for a fundamental reevaluation.

If CoCom-era controls were eliminated, three sets of controls will still apply to exports of information technologies. Munitions controls will apply to systems and software specially developed for military purposes. Work by the Department of Defense recommends that munitions controls focus on critical national security applications developed specifically for the military and that the United States use additional techniques (such as software protection technologies) to safeguard these applications.

For general-purpose information technology, the most important authority the United States will retain is its “catch-all” control—EPCI. “Catch-all” controls, as their name implies, apply to any export when the intended recipient is a proliferation-related entity. EPCI controls will continue to allow the United States to stop U.S. firms from exporting information technologies at all performance levels to proliferators without the need for MTOPS-based controls.

The United States created EPCI in response to Iraqi efforts to acquire items in the United States for use in WMD facilities. The multilateral nonproliferation regimes did not control these items, and the licensing process could not stop their export, so the normal process of export controls was ineffective in stopping them. The solution to this problem was to create “catch-all” controls in 1990. EPCI, an essential authority for the United States, applies to both goods and services and should remain an essential element of export controls on information technology.

EPCI has three elements. First, it allows the government to stop any shipment of any item going to questionable end-users for proliferation-related purposes. Under EPCI, the United States can impose licensing requirements on exports and reexports of normally uncontrolled goods and technology where there is a risk of diversion to WMD or missile proliferation. This remains as important

EPCI controls should remain an essential element of export controls on information technology.
EPCI allows the US to:

1. Stop the export of any good for proliferation purposes.
2. “Inform” an exporter that sales to a foreign entity will need a license.
3. Require an exporter to screen potential export to avoid transfers to WMD programs.

as it was in the early 1990s.

Second, EPCI gives the United States the authority to “inform” an exporter that a foreign entity is ineligible to receive U.S. goods without prior approval. The informing process can occur through a letter either to the U.S. exporter or through publication of an entity or list of entities in the Federal Register Notice. Once the United States lists an entity, exporters must obtain a license before selling to these entities. This authority also remains essential.

Finally, EPCI requires exporters to screen potential sales to avoid transfers to WMD programs. Exporters must apply for a license whenever they “know or have reason to know” the export could be associated with WMD-related activities. Screening is the least effective part of EPCI and the part most in need of repair. Improved EPCI screening requires a more focused approach to countries and items and a greater flow of information from the government to exporters.

The raison d’être for EPCI is that the government has knowledge about a potential diversion to a WMD-related activity that the exporter lacks. The provision of information on proliferation projects to exporters should be the cornerstone of EPCI, but the somewhat formalized EPCI process that has grown up in the last decade is inadequate at supplying the names of entities of concern. There are several methods for expanding the transfer of knowledge about proliferators from the government to the private sector.

The primary vehicle for providing exporters with information about end-users of concern is the Entity List, which is published in the Federal Register. The current Federal Register process at times seems better suited to limiting information available to exporters than providing an adequate list. Intelligence experts agree that 200 to 300 entities in perhaps a dozen countries are directly involved in WMD proliferation. Without counting those entities placed on the list by sanctions on India, the Entity List has approximately 50.44

The chief problem with expanding the U.S. lists lies with interagency coordination. The Intelligence Community seeks to protect sources and methods, and the State Department seeks to protect diplomatic relations. The sources and methods problem can usually be resolved. Diplomatic concerns are more difficult. Publishing the “Entity List” in the Federal Register ensures diplomatic problems and limits the government’s ability to provide timely or adequate information on proliferators.

The existing process has become unwieldy and should be buttressed with additional processes for information sharing. These processes should include expanding the entities list to a credible number, broadening agencies’
outreach activities on proliferation, and altering the “is informed” process to increase dissemination of questionable recipients. To reinforce the Entity List, the United States could add names taken from other public lists. The UK’s Department of Trade and Industry has an Entity List that is more complete than the U.S. list for some countries. The list is not published, but is provided to exporters on an official basis. U.S. agencies could use this list as a source for additional entities.

An expanded “is informed” process is also necessary. When one exporter “is informed” that there are proliferation concerns with a potential customer, greater effort should be made to inform all potential exporters. Currently, when an exporter has concerns about a potential customer, it inquires to the Department of Commerce as to whether there are proliferation concerns with an entity. Commerce responds in writing to say that a license is required. Other exporters may not have the same concerns and may not inquire. One U.S. computer company reports that it made an inquiry about an entity, and Commerce replied that there were concerns. A competitor, unaware of these concerns, went ahead and made the sale. Because no one had informed the competitor and it had exercised due diligence in screening, the export was legal. The current system can act to penalize caution.

Fixing this requires sharing “is informed” information on proliferation-related entities as broadly as possible. Commerce should notify not only the company that made the inquiry but other U.S. suppliers as well. Some computer firms use direct sales and others rely more on distributors, creating an extra burden in this expanded notification process, but this is not an insurmountable difficulty.

The “is informed” process could also take advantage of Web-based technologies. Entities identified through the “is informed” process could be listed on Web sites. Agencies could use software applications that would allow companies to submit names and addresses for automatic screening. Sales representatives and exporters could enter a name and address of a potential customer and get an immediate response as to whether there were EPCI concerns. For information technologies and other items, agencies should explore how to work with trade associations to take advantage of their communications networks that link members to provide information on suspect transactions. This could reach a broader and more complete group than the current practice. Some argue that this process would not reach all potential exporters and therefore should not be used. It seems better, however, to reach 8 people out of 10 than to reach none out of 10.

Companies could improve their screening of potential buyers if the United States used lists of items and countries focused on real proliferation concerns. The United States has struggled for a number of years to develop a “positive
list” that would identify a specific list of items that would need to be screened. The closest agencies have come to implementing such a list was in the regulations published in 2000 that eased sanctions on North Korea. These regulations identified items not controlled by the multilateral nonproliferation regimes that would still require a license for export to North Korea. The United States created several new entries on the Commerce Control List to capture production equipment and software exports to North Korea. This Korea list, which reflects missile and nuclear proliferation concerns, could form the basis for a positive list for EPCI.

The United States could focus the list of countries that require screening onto those countries where it has proliferation concerns. The CIA identifies Iran, Iraq, North Korea, Libya, Syria, Sudan, India, Pakistan, and Egypt as countries acquiring WMD technology. DOD’s list adds China. Commerce’s Entity List includes Israel. Screening would be more effective if applied to a targeted list composed of these countries rather than to the 40 or so countries for which screening is now required.

EPCI authorities remain essential for the United States to be able to regulate exports in its national interest. Information technologies pose an anomaly—as computing power become ubiquitous, the United States can no longer reasonably expect to deny access by proliferators. That said, it would want to ensure that U.S. companies do not directly contribute to foreign WMD projects.
Chapter 4
Computer Technology and National Security

“Advantages will go to states that have a strong commercial technology sector and develop effective ways to link these capabilities to their national defense industrial base.”
—Central Intelligence Agency, “Global Trends 2015”

The centerpiece of the revolution in military affairs is the shift from weapon-centric warfare to network-centric warfare. Many efforts are under way to incorporate information technologies into military operations. Future military operations will involve extensive networks of sensors, databases, command, control, and analytical capabilities that provide information directly to the warfighter and to smart weaponry on an immediate, real-time basis. Computing and network innovations will allow for seamless, real-time connections between troops, sensors, command, platform, and weapon. Data from sensor platforms such as remote sensing satellites or unmanned aerial vehicles, automatically processed and referenced against existing databases located hundreds or thousands of miles away, could be communicated directly to soldiers, platforms, and intelligent weapons. The physical dispersal of forces need not degrade command and control, and maneuver and targeting capabilities can be enhanced and accelerated.

The more flexible and precise military force that the United States could develop using information technology would have an advantage in the new international security environment. Maintaining U.S. superiority requires taking a number of steps: forming partnerships with the information technology industry and academic community; creating a process to increase the flow of innovation and to change doctrine and practices accordingly; and building a strong foundation of education and research to ensure that U.S. technology is as advanced in 10 years as it is today.

Partnership with the private sector is a “new” tool for governance that the United States has already begun to use in areas like encryption policy and critical infrastructure protection to address national security problems where the private sector has an equal role to play. Vehicles for partnership include new, focused advisory groups, task forces, and exchange programs for DOD personnel at information technology companies, internships, and the establishment of joint research programs. The broad objective should be to create connections between the government and the private sector that match warfighters’ needs and private sector innovations. Ideally, DOD warfighters and private sector technical personnel (including chief technical officers)
could work together to improve U.S. capabilities.

Creation of a joint evaluation center, staffed with both government and industry detailees to look at technologies and applications either in development or planned for development, would help the United States better understand, and adjust to, the new global technological environment. As a related measure, the United States might want to expand existing programs at the National Defense University (NDU) and other military education facilities. Existing efforts at NDU and the War Colleges could be reinforced by additional programs and faculty staffed by technologists from the information technologies industries. The United States may also want to integrate private sector information technology expertise directly into facilities like the Army’s National Training Center for the development of new doctrine and tactics. Private sector experience may not translate directly to the military and government, but the experience of applying new information technologies to global companies and the effects this had on organizations could be valuable for guiding changes in the national security community.

New technologies are not a panacea—they must be accompanied by doctrinal and organizational changes to reap their full benefit. The French had better, and more, tanks in 1940 than did the Germans, but the Germans used their tanks in new ways. The United States, given the strength of its industry, will have greater opportunities than its potential opponents to gain the advantage if it can find ways to use these technologies to transform processes rather than merely injecting them into existing processes. The most immediate example of this would be logistics and acquisitions reform at the Department of Defense. The private sector has made advances in improving supply chain management and acquisitions that the national security community could mirror. Using B2B (business-to-business) models would streamline acquisitions activities.

The creation of a business-to-business portal by General Motors Corporation, Ford Motor Company, and DaimlerChrysler is a useful model for DOD. This experience of large competitive bureaucracies working together could map well to DOD and the armed services. The three companies formed a business-to-business integrated supplier exchange through a single global portal. It is an online global network that provides for catalog purchasing, bidding and price quotes, online sourcing, and auctions. In addition, it provides supply chain management functions such as capacity planning, demand forecasting, production planning, transaction automation, financial services, payment, and logistics. The companies were able to set up this supply chain network quickly and without putting sensitive information at an unacceptable risk.

Improved logistics and acquisitions processes will help address the problem
of DOD’s information technology often lagging behind the private sector in information technology. Using old technology can be expensive, as models go out of production and spare parts and maintenance costs increase. Adopting B2B (business to business) practices can allow DOD and the armed services to have a faster “refresh rate” for information technology. Solving this problem will require changes in funding and acquisitions practices, but it will also require using technologies incorporating open systems and standards and “plug-n-play” technologies by DOD, to allow easier upgrading of systems.

Partnerships with the private sector that can increase the flow of innovation to the national security community will require changes in acquisition practices and a devolving of acquisition authority to the “customer” rather than some intermediary, or complex, hierarchical review process. Existing acquisition practices are a disincentive for innovative information industry companies. Although Defense contractors have mastered the complex defense acquisition system, information companies whose primary market is global and civil may find the opportunity cost of working with DOD on specific applications too high. The leading innovators are not defense contractors and are unwilling to absorb the costs of learning how to sell to DOD; they can make as much money or more selling to the commercial market. Acquisition regulations may be the biggest obstacle to greater use of information technologies. Congress and the administration need to change the acquisitions process to allow the United States to gain the full benefit of its lead in commercial technologies.

Some problems of interest to the national security community (global operations and logistics, acquisitions, purchasing, data mining) have already gone through several iterations in the private sector. The United States can capitalize on these experiences. DOD and the private sector could explore these commercial innovations now for projects of national security benefit. As first step in translating these concepts in practical tools, DOD or DARPA might wish to begin four or five fast-track programs with leading information technology companies to develop new applications. Possible fast-track program areas include:

—Wireless broadband applications. The military is likely to be one of the most avid consumers of wireless broadband applications. These applications can help solve the “last mile” problem by greatly extending data and communications networks. One commercial model, for example, uses a low earth-orbit satellite network to provide data transfer rates of up to 200 kilobits per second to aircraft. The Global Broadband System (GBS) and its predecessor the Joint Broadband System offer existing platforms for the integration of new technologies. Other commercial products in development (such as those using Bluetooth or other short-range, secure wireless
standards) could also be applied to military applications.

—**Pervasive computing/embedded intelligence.** Cheap, powerful CPUs and specially designed operating systems and applications can be incorporated into ships, aircraft, vehicles, and facilities, creating dense networks of “intelligent” devices. These devices could automate functions and provide a more detailed and complete situational awareness. Managing the floods of data generated by these dense networks of intelligent devices will itself have to be automated, using software agents, data mining, and other applications. Pervasive computing and network technologies would enhance redundancy and improve communications across commands, and artificial intelligence functions could improve computerized pattern recognition to allow automated rules of engagement, rapid assignment of weapons to hundreds of targets, and some automated maneuver and logistics functions.

—**Software agents, or “bots.”** Bots are software tools for retrieving and managing information from remote sites on the network. Defense has a number of projects already under way to exploit software agents. These tools can perform statistical analysis, resource discovery, network maintenance, and updating and can provide “mirroring” of information. More sophisticated bots can be self-configuring and can make decisions on how to refine searches based on their own search experience.45

—**Data mining.** Database applications that automatically search for new patterns or new relationships in a large amount of data offer possibilities for improved intelligence functions, maintenance, personnel, and other activities. Combined with software agents, data mining would enhance and accelerate the tasking, processing, evaluation, and dissemination (TPEDS) process used in the intelligence community.

—**Collaborative virtual workspace.** Group-to-group communications networks can bring people together in real time, regardless of their physical location, for large-scale distributed meetings, collaborative work sessions, and training, using large-format displays and “intelligent” meeting rooms.

**Education, Research and Development**

Enhancing national security with new information technology also requires addressing fundamental problems in education and long-term research and development. The United States faces a shortage of skilled workers in the information technology sector. This shortage has worsened in recent years, particularly in the government, where organization and pay scales put it at a disadvantage in competing for skilled information technology personnel. The general shortage means that information technology workers are expensive, making it difficult to staff positions at government salaries—particularly at
entry levels. The private sector can overcome this shortfall by recruiting skilled labor from foreign countries, but this does not work for national security applications. The United States needs to find the incentives and develop the programs that will produce an adequate supply of information technologists. One solution is to adopt a scholarship model where the United States would pay for higher education in exchange for a commitment to service for a number of years, as is already done with other short-supply skills such as medical care.

Maintaining U.S. superiority also requires addressing the long-term problem of funding research and development. The United States needs to ensure that the pipeline of innovation does not run dry, as that would eliminate an important element of U.S. superiority. This expansion should apply to research both in specific information technologies and in the basic research that underpins developments in information technologies. Basic research funded by DARPA and others in the 1970s and 1980s underlies much of the progress made in information technology in the past two decades. This kind of long-term investment must be repeated to maintain U.S. superiority.

Attention to the fundamentals (education and research and development) is essential for the United States to protect its national security in the face of challenges from potential opponents. Other nations are deeply interested in the use of information technologies to gain “asymmetric” advantage over the United States. Export controls do nothing to help manage this risk, as they cannot catch the technologies involved. An increased pace for innovation by the United States, however, will make it harder for potential opponents to benefit from asymmetric approaches. Although the United States is perhaps the nation most vulnerable to cyberattack, it is also the best positioned (given the size of its industry and its defense establishment) to exploit new technologies to its advantage, including in information warfare.

Potential opponents will also face a more difficult task if the United States pays sufficient attention to information security. To some extent, this is a question of making strong, well-designed interoperable encryption an integral part of national security applications. Progress is also necessary in critical infrastructure protection and information assurance efforts. Some efforts are already under way at Defense, such as DOD’s Public Key Infrastructure (PKI) for its own network. The United States has made progress in protecting its critical infrastructures, but the task is not complete. Information technologies can strengthen U.S. military forces’ ability to operate in physical dimensions, but the United States also needs to ensure that U.S. cyberspace capabilities match the deterrent and defensive capabilities of U.S. strategic and conventional forces.

As part of this, the United States also needs to expand its ability to assess
what other nations’ forces can do with commercial technology and widely available military technology. It could perhaps use joint military/private sector evaluation centers and industry partnerships to counter attempts to gain asymmetric advantage by developing DOD programs and initiatives.

Developing and strengthening partnership with the information technology sector requires finding new vehicles that differ from the traditional relationship with a “contractor” and to make the changes in organizational structures and procedures that would allow and accelerate these partnerships. These partnerships are central, as the bulk of innovation and development of applications and networking technologies is taking place in the private sector. There is a precedent for this—the resolution of the debate over encryption is one such model. It will not be possible to turn information technology companies into defense contractors (and it is not in the national interest to do so), but there are ways to build cooperative relationships that provide benefits to both.
Chapter 5

Conclusion

The United States now faces complex challenges in a world that has changed significantly since the 1980s. Regional conflicts, terrorism, and the proliferation of weapons of mass destruction threaten U.S. national interests. A global economy and the spread of information and technology throughout an increasingly competitive world marketplace create new challenges for U.S. national security.

Research and manufacturing capabilities for information technology are now global. Access to technology and technical capabilities has spread widely and continues to spread in a global market. Barriers to entry for new competitors in information technology tend to be economic rather than technological. The United States leads in many technologies, but it does not have a monopoly.

The current system of computer export controls derive from an era when U.S. strategy was to deny the Soviet Union access to technology. Limited communications, allied cooperation, and the real threat posed by the Soviets made this effective. Now, MTOPS-based hardware controls are increasingly irrelevant, given the lack of multilateral cooperation, the spread of technology, increases in computing power with more capable microprocessors, and the development of alternative sources of supercomputing like clustering and network computing. Computing power is becoming ubiquitous, as more devices contain processing power equal to what was once considered a supercomputer. Access to computational power continues to expand with technological advances and the spread of the Internet.

Consensus between the United States and its allies on threats and technology transfer has eroded. Multilateral cooperation for controlling information technologies is at a low ebb. The Wassenaar Arrangement, which controls general-purpose computers, has been decontrolling information technology since its inception. Wassenaar computer controls are set at a level far above what military applications need, and Wassenaar members will not embargo civil technology to countries like China or India. The absence of a common security threat and the emergence of a competitive global market mean that there is no support for Cold War controls on computers.

Computing power is not itself a chokepoint for military and proliferation activities. Computers of 500 to 1000 MTOPS are sufficient for military and proliferation purposes. Specially developed software codes, extensive databases, and the manufacturing and integration skills necessary for modern weaponry are more important. Military power today depends not only on the tools of the industrial age but on the tools of the information age as well. Potential opponents will seek to exploit U.S. vulnerabilities with the new technologies. The United States will need to find ways to use advanced commercial technologies to improve military capabilities and work with the private sector to enhance U.S. security. For the United States, information technology, properly integrated into battlefield operations, can provide the margin of victory.
All of these developments will erode U.S. national security unless the United States takes steps to adjust its policies to the new situation. Denying access to computing power, although strategically important in the 1980s, is now ineffective and even counterproductive. The issue must now be recast. The new administration and the new Congress have the opportunity to take the bold, necessary steps needed to advance U.S. national security.
Appendix A

MTOPS and Its Alternatives

MTOPS. The rationale used in the White House High Performance Computer announcements of January 2001 set control levels for MTOPS (millions of theoretical operations per second) based on the MTOPS levels produced by different combinations of processors. This method requires constant control-level updates as microprocessor technology improves and companies release chips with even better performance measures. Some suggest that the MTOPS calculation be rejiggered to look at billions, rather than millions, of operations. Then 85,000 MTOPS would become 85 BTOPS—a mere cosmetic change that fails to address the real problem with MTOPS.

MTOPS levels for individual microprocessors appear to be rising rapidly, in part because some companies place capabilities on a single microprocessor whereas other companies put these functions on two processors. The result is that although the first company’s chips will have drastically higher MTOPS than the other companies’ chips, their performance capabilities are the same. If MTOPS continue to be used in current form as a metric, systems that have the same performance capabilities will be treated differently under the regulations.

Power dissipation. The power dissipation ratio measures watts per MTOPS in relation to the size of the box housing the microprocessor. (Japan uses power dissipation to determine the environmental effects of computers.) Power dissipation does not accurately measure the performance capabilities of a system. Two systems can have the same performance capability, but because one is in a larger box with a larger power supply and more disk drives, it will have a lower power dissipation ratio and would therefore be controlled less stringently. This method could also encourage people to evade export control by simply placing their systems in larger boxes.

Linpack benchmark. Linpack, one of several floating-point benchmarks, is named after a linear algebra package that it uses to solve linear equations. This benchmark is used to determine the performance of systems on the list of Top500 Supercomputer Sites (www.Top500.org). The performance numbers give a good estimation of peak performance. Although Linpack is an accepted industry standard for performance measurement, several reasons preclude its being used as an export control metric. A computer’s performance can change over time as the compilers and operating system change—Linpack measures both hardware capabilities and associated software. If the software changes, the Linpack metric could also change. Once the system is with the end-user, the end-user could change the software and upgrade the system.

Memory bandwidth. Memory bandwidth, which measures the ability of a computer to pass data from a processor to memory, is an indicator of performance. Currently, most commercial CPU’s have a low memory bandwidth when contrasted with true “supercomputers”—vector machines made by companies like Cray or Fujitsu. Moving to a memory bandwidth metric would release most commercial systems, but it could be difficult to win multilateral agreement to this metric as it would release U.S. computers and catch those built by other countries.
**Processor count.** Processor count would control computers based on the number of CPU microprocessors they contained. A processor-based control matches the rationale used in the White House High Performance Computer announcements of 1999 and 2000, which set licensing thresholds by estimating the MTOPS of computers using 4, 8, 16, or more processors. A processor count metric would avoid the need to constantly update regulations to consider new, higher-powered chips. The United Kingdom proposed in April 2000 that the Wassenaar Arrangement replace MTOPS with a processor count metric, because it would release the majority of digital computers used for nonstrategic (office) applications. The UK proposal was set aside for further study, as a computer using many low-powered chips could be caught, while a more powerful computer using a few, high-powered chips would be released.

**MFLOPS.** MFLOPS, or floating-point operations per second, is a standard measure of processor speed and a method of encoding numbers that can process extremely large numbers relatively easily. The computation of floating-point numbers is often required in scientific or real-time processing applications, and FLOPS is a common measure for any computer that runs these applications. MFLOPS is millions of floating-point operations per second. GFLOPS is billions of operations. The performance of the most powerful computers (and those that may still justify control) is measured in teraflops—that is, trillions of floating point operations per second. Compaq is assembling a computer for the Department of Energy that will operate at 30 teraflops. The National Science Foundation is working on a “grid” of networked computers that will provide researchers with remote access to computing power measured in petaflops—a thousand trillion floating-point operations per second.47
Notes

4 The National Science Foundation estimates that although the United States continues to have the largest share of the high-tech market, its actual share has dropped from roughly 25 percent to 18 percent as new economies, especially in Asia, entered the high-tech market. National Science Foundation (NSF), Science and Engineering Indicators 2000 (Washington, D.C.: NSF, 2000).
8 Information provided by IBM.
9 William Van Loo, chief technologist, computer systems, of Sun Microsystems, Inc., wrote in a personal communication: “Google provides a very sophisticated search engine service as well as search engine software technology. Their search engine service is run on racks of servers, all small Pentium machines running Linux. Their business depends on accessing storage—massive, cheap storage—and assembling a response to a search query from parallel access to multiple machines—typically more than 50 machines per query. What surprised even me is how they built up their racks of servers. A standard rack is measured in Rack Units (RU) and is 42 RU high. This rack today contains an Ethernet switch in the middle and 20 server boxes, each 2RU high. This server box contains: 2 Pentium processors at 500–600MHZ, 2 IDE disks at 30GB–40GB per disk, 4 memory DIMM slots, typically filled with 2GB of ECC memory. This configuration is not surprising. What I found surprising, though, is that they design and contract assemble these boxes themselves. They buy standard motherboards, low cost Pentium processors, spot market memory DIMMs, and IDE disks, and have the boxes assembled at a foreign assembly plant. Finally, it takes fewer than 10 engineers to design each generation server box; a new generation is introduced every 6 months. Since these designs are for internal use, they do not care about margins—100MHZ ECC memory DIMMs are run at 133MHZ, for example. If a few boxes arrive and they do not work, they are thrown out. Google shows that the specter of low cost server racks built from commodity parts is no illusion. There is nothing in their assembly process that can be controlled for export.”
11 Top500 Supercomputer Sites’ annual review of supercomputers for 2000 concluded that “the availability of relatively low-cost (RISC) processors and network products to connect these processors together with standardized communication software has stimulated the building of home-brew clusters computers as an alternative to complete systems offered by vendors.”


14 “Beowulf,” for example, is software created to allow smaller colleges and universities to use their computer networks to obtain high performance computing. It can be downloaded from the Internet.


16 Juno, an Internet service provider, is a prominent example.


18 Central Intelligence Agency (CIA), Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 2000, July 2000. In a similar vein, David Albright wrote in the June 1993 Bulletin of the Atomic Scientists, “Stringent export controls have slowed nuclear weapons efforts, and bought time for political approaches to work. By denying modern computerized manufacturing equipment, for example, export controls can force clandestine programs to rely on less sophisticated machine tools. These machine tools usually produce items more slowly and require more skillful operators, who are often in short supply in developing nations. But export controls are not a panacea. A determined country with adequate resources can mount an effort to defeat or bypass export controls. Because technology is spreading worldwide, export monitoring may eventually become less effective.


22 Ibid., 15.


28 Cooper, “Military Working Group Paper.”
29 The Rock Island Arsenal, working as a test bed for DARPA in advanced military productions, found it could run the most sophisticated software “agents” for modernized production methods with a handful of Pentium desktop computers. The project reports, “It is substantially less expensive from a hardware perspective to use a large number of inexpensive processors than a single processor having equivalent total processing capabilities. See Autonomous Agents at Rock Island Arsenal, http://www.aaria.uc.edu/menu.html, accessed April 15, 2001.

30 Statement by Congressman Christopher Cox, press release, April 24, 2001, on CSIS/Stimson Center report, “Study Group on Enhancing Multilateral Export Controls.”

31 The appearance of the Organization for the Prevention of Chemical Weapons (OPCW), the operational arm of the Chemical Weapons Convention, has complicated the fate of the Australia Group.

32 MTCR does control computers specially designed for use on missiles. This control does not apply to the commercial computers sold by the information technology industry.


34 No Wassenaar member has reexport requirements like those used by the United States, and most Wassenaar members regard U.S. reexport controls as intrusive and extraterritorial. This means that unless the United States is willing to stop selling to Europe and Japan, it cannot expect to prevent the resale of information technology to places like Iran and China.


36 Export Administration Regulations Section 740.xx.

37 GAO, Export Controls, 5.


40 Cooper, “Military Working Group Paper.”

41 Ibid.

42 Ibid.

43 Iraq sought to purchase a high-temperature “skull” furnace from a U.S. manufacturer, allegedly for use in making prosthetic devices for veterans of the Iran-Iraq War. Skull furnaces were not controlled for proliferation reasons; the United States had no authority to stop the shipment. Although the export was finally prevented, the difficulties in doing this led to the creation of EPCI authorities.


45 There is abundant literature in military periodicals on this point. A recent recommendation would be, for example, the 2000 Report of the Independent Commission on the National Imagery and Mapping Agency (“The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Environment,” December 2000) which says: “NIMA should aggressively explore ways to realize the large potential for improving effectiveness through ‘force multiplier’ opportunity in automated extraction tools or both geospatial and image analysis.”

46 Examples include SIMD (Single Instruction Multiple Data—a data processing standard that speeds performance) and MMX (Multi Media Extension—a SIMD extension that accelerates calculations for audio, video processing, voice synthesis, and 2D and 3D modeling).

accessed May 1, 2001.