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[1]

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.

The multilateral framework for export controls consists of the Nuclear Suppliers Group, the Missile Technology Control Regime, the Australia Group and the Wassenaar Arrangement

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.[2] 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.[3] 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

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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.

Disputes between the US and its partners in the Wassenaar Arrangement are frequent, reflecting wide disparities in foreign policies.

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 members argue that information technology is now a routine part of 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.[4] 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.

Despite U.S. objections, Wassenaar has turned from controlling hardware controlling production equipment and technical expertise.

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.[5] 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.[6]

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.[7]

Japan has asked to terminate the bilateral agreement with the US on supercomputers because it no longer has any strategic relevance.

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.

In the current climate of very limited multilateral cooperation, the U.S. would be hard-pressed to keep information technology out of the hands of potential opponents.

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.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

The Question of MTOPS

"MTOPS is an outdated measure…."
—General Accounting Office[8]

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 ineffective as a measure of performance

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

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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."
>
> —William Owens, "The Emerging U.S. System-of-Systems"[9]

The widespread availability of computing power is part of a larger trend identified by the Defense Science Board Task Force on Globalization[10]—the global diffusion of technology. This trend could degrade U.S. national security unless the United States takes effective in response.

Potential adversaries hope that information technology could allow them to disrupt U.S. power projection capabilities.

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.

The U.S. could face greater risk from network vulnerabilities than it does from any potential contribution of high performance computers to proliferation.

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

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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."[11]

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.[12] 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.[13]

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.

Post-CoCom Export Controls

The U.S. controls general-purpose computers with a complicated and ineffective system of MTOPS levels and country tiers.

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,

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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.

EPCI controls should remain an essential element of export controls on information technology.

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.[14] 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 ands 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 as it was in the early 1990s.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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.**

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'etre 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.[15]

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

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

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.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

Notes

[1] Statement by Congressman Christopher Cox, press release, April 24, 2001, on CSIS/Stimson Center report, "Study Group on Enhancing Multilateral Export Controls."
[2] 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.
[3] 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.
[4] Institute for Defense Analyses, Wassenaar Negotiations, Volume 3 (1998).
[5] 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.
[6] See, for example, Richard T. Cupitt, "Control Regime Working Group Paper," prepared for the CSIS Information Technology Export Control Project, December 29, 2000.
[7] Export Administration Regulations Section 740.xx.
[8] GAO, *Export Controls,* 5.
[9] William A. Owens, "The Emerging U.S. System-of-Systems," *Strategic Forum* (National Defense University), February 1996.
[10] Defense Science Board, *Final Report of the Defense Science Board Task Force on Globalization and Security*.
[11] Cooper, "Military Working Group Paper."
[12] Etter et al., "Export Control of High Performance Computing," 6.
[13] Ibid.
[14] 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.
[15] See U.S. Department of Defense, "Proliferation: Threat and Response," January 2001; CIA, *Unclassified Report to Congress on the Acquisition of Technology;* Wisconsin Project on Nuclear Arms Control, "Country Info" (February 22, 2001), http://www.wisconsinproject.org/, accessed April 15, 2001.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.