
**ARMS CONTROL, EXPORT REGIMES, AND
MULTILATERAL COOPERATION**

Lynn E. Davis

In the past, arms control, export regimes, and multilateral cooperation have promoted U.S. security as well as global stability. Vast stockpiles of weapons have been eliminated. Destabilizing nuclear systems have been banned. Confidence-building measures have enhanced security in Europe. Various treaties and export-control regimes have prevented the spread of weapons of mass destruction and sophisticated conventional weapons. Multilateral cooperation agreements have been used to prevent common threats, such as nuclear smuggling.

The question is whether any of these approaches—arms control, export regimes, multilateral cooperation—can serve U.S. security and global stability in the future in connection with the development and deployment of information-warfare systems. The obvious problem, which other chapters in this book describe, is that so much uncertainty still surrounds this whole subject. Many of the information systems and technologies are just beginning to be designed. Still unclear is an understanding of the kinds of threats that will emerge both to American society or to the U.S. ability to employ its military forces. No one knows who will be able to develop or acquire these new systems and in what time frame. So the strategic assumptions that will guide U.S. policies and strategies cannot be defined. Nevertheless, it is not too soon to begin to consider this question, and this is the purpose of this chapter.

This chapter begins with a description of some of the past accomplishments of arms control, export regimes, and multilateral cooperation. It then turns to what this history suggests for the role that each of these might play in the age of information warfare. Important to future decisions will be one's strategic assumptions about

whether the United States will be able to maintain superiority in information warfare and how widely disseminated information-warfare capabilities will be. The chapter considers various possibilities and then defines some of the issues that will need to be addressed, if any of these three approaches were to be pursued. The chapter concludes by defining the tasks the United States should undertake during this time of uncertainty, so as to prepare for the possibility that arms control, export regimes, and multilateral cooperation might play a critical role in the age of information warfare.¹

PAST ACCOMPLISHMENTS

Arms Control

During the Cold War, the United States and Soviet governments viewed arms control as a way to promote strategic stability and reduce the threat posed by the accumulation of strategic nuclear arms; with European governments, they saw arms control as the means to ameliorate the threat arising from the massing of conventional armaments in Central Europe. In the 1970s, arms control had some limited success in promoting these goals. The Antiballistic Missile Treaty banned nationwide strategic defenses, and the Strategic Arms Limitation Treaty agreements capped the overall levels of Soviet and American strategic nuclear delivery vehicles. The Helsinki Final Act of the Conference on Security and Cooperation in Europe (CSCE) included principles upon which to conduct relations, as well as some rudimentary confidence-building measures.

As cooperation began to replace confrontation, with the fall of the Berlin Wall and the dissolution of the Soviet Union, arms-control negotiations made more-significant progress. The CSCE countries agreed in the Stockholm Document to confidence and security-building measures that were designed to reduce the risks of war through surprise attack and misunderstanding in a crisis. The Strategic Arms Reduction Talks (START) treaties mandated major reductions in the number of strategic nuclear missiles and bombers.

¹The author wishes particularly to thank Jeremy Shapiro for the many ways in which he supported the writing of this chapter, and especially his wise counsel. Thanks as well to Robert Nurick, whose very thoughtful and insightful review improved the argument.

The Conference on Forces in Europe (CFE) Treaty produced equality between the North Atlantic Treaty Organization (NATO) and the Warsaw Pact in the most-dangerous conventional weapons, tanks, artillery, and armored personnel carriers. Confidence-building measures were expanded and improved through the 1988 Charter of Paris and the 1994 Vienna Document.

In 1997, the United States and Russia agreed to guidelines for a START III treaty, which will lower further the overall number of strategic missiles and bomber weapons and provide for new measures that will increase the transparency of their strategic nuclear warhead inventories and require the actual destruction of the nuclear warheads themselves. The CFE Treaty will be adapted over the next few years based on a framework, agreed to in the summer of 1997, that calls for further reductions in conventional weapons, as well as measures to prevent any threatening buildup of conventional forces in Central Europe. The NATO Founding Act of May 1997 envisions a role for arms control in enhancing security in Europe as NATO expands, through confidence-building measures built on exchanges of information on military infrastructures throughout Europe.

In 1995, the Nuclear Non-Proliferation Treaty, in which some 170 countries have agreed not to acquire nuclear weapons, was extended indefinitely and unconditionally. One of the ways that the nuclear powers gained the support of the nonnuclear states to the extension of the Non-Proliferation Treaty was to commit, through arms control, to further reductions in their own nuclear weapons. They also provided "security assurances" to the nonnuclear states relating to the circumstances when they would and would not use nuclear weapons in the future. Arms control has also produced agreement for the destruction of all stockpiles of chemical and biological weapons and the prohibition of any future development. The Chemical Weapons Convention and the Biological Weapons Convention became possible once the parties recognized that these weapons were not very useful militarily and posed a serious threat if used by others.

This brief history demonstrates that arms-control negotiations can achieve a variety of different goals and that governments have been extremely creative in tailoring various measures to respond to the specific characteristics of the threats and the individual weapon sys-

tems. The parties to these arms-control agreements have been nation-states, given their responsibility for deploying and operating the weapon systems. The ability of governments to verify the limits confidently has been a critical element, although the standards of verification have been somewhat relaxed as the threats have diminished.

Measures to build confidence and security proved to be possible, even when only the most minimal cooperation existed among the parties. As cooperation expanded, governments found arms control a useful way to move mutually to lower levels of armaments and even to eliminate reciprocally whole classes of weapons: intermediate-range missiles in Europe and strategic missiles with multiple warheads. They were also prepared to undertake reductions, through reciprocal—but unilateral—steps, and thereby forgo intrusive verification procedures, as in the case of theater nuclear weapons in Europe.

But there have been important limits to what arms control has been able to accomplish. The newest weapon systems have not been banned, even in the case of antisatellite systems, when neither side saw any advantage in their actual deployment. To retain their own military flexibility in a crisis, governments have resisted strict limits on their military activities and deployments, even though limits might have eliminated the threat of surprise attack.

Export Control Regimes

Historically, the industrialized nations have taken a variety of steps to keep dangerous weapons, as well as the means to develop such weapons, out of the hands of enemies, especially rogue states and terrorists. During the Cold War, the NATO countries, joined by the neutral countries in western Europe, restricted the transfer of all conventional weapons and related technologies to the Soviet Union, China, and North Korea, through the Coordinating Committee for Multilateral Export Controls regime. In this case, the threat was unambiguous and extremely serious.

With the end of the Cold War, the security threats became more diffuse. But governments saw dangers in the spread of dangerous weapons and undertook to establish international norms against the

proliferation of weapons of mass destruction, long-range missiles, and sophisticated conventional weapons. To reinforce these norms, multilateral export regimes were established to control transfers of each of these weapons and their related technologies.

The Nuclear Suppliers Group, composed of 30 suppliers, has established guidelines and controls for exports of nuclear materials, equipment, and technologies. The Australia Group is an informal arrangement among most of the industrial countries that reinforces the Chemical and Biological Weapons Conventions by preventing transfers of certain kinds of chemical and biological weapon material and dual-use technologies.

The Missile Technology Control Regime (MTCR), established in 1987, seeks to control exports of equipment and technology, both military and dual-use, that could contribute to missile development, production, and operations. To prevent buildups of destabilizing conventional weapons, as occurred in Iraq, over 30 of the major suppliers of conventional weapons have joined together in the Wassenaar Arrangement to promote transparency and restraint in sales of conventional weapons and related dual-use goods and technologies.

These regimes control exports to both nation-states and non-governmental groups. They cover weapons and the equipment and technologies that are necessary to develop the weapons. Each of the regimes includes a list of the weapons, equipment, and technologies that are to be controlled; rules governing their transfer; and a commitment to report on licenses that have been approved and denied.

These regimes have been designed in light of the unique characteristics of the weapons they cover. Given the extremely serious threat posed by weapons of mass destruction, these export regimes include rules that generally “ban” any transfers of the listed equipment and technologies. The MTCR members view the long-range missile proliferation threat as sufficiently serious to warrant rules that presume that all transfers of the listed items will be denied to non-MTCR countries.

Conventional weapons are different, for all nations consider them essential to their own defense. A threat arises only in specific circumstances, when weapons are acquired by rogue states and terror-

ists, or when the introduction of new weapons upsets a regional balance. So members of the Wassenaar Arrangement have been reluctant to coordinate their policies on conventional arms sales or to commit to specific rules governing their transfer. They do, however, each have national policies prohibiting transfers of conventional weapons and military-related technology to Iran, Iraq, Libya, and North Korea.

Even when the political will exists among governments to prevent the spread of dangerous weapons, many obstacles exist. The United States, Japan, and western European countries have fairly sophisticated systems for implementing export controls, but other countries are just beginning to put theirs in place. Most of the goods on the control lists have legitimate civil, as well as military, uses. So governments must create licensing procedures that permit legitimate sales but prohibit dual-use goods from being diverted to dangerous military uses. This is especially difficult in the face of an adversary determined to circumvent the controls.

Strong commercial interests exist in every country for expanding trade in dual-use equipment and technologies, leading to pressures on individual governments to remove items from the control lists. Countries strike different balances between their commercial and nonproliferation objectives. The United States liberalized its trade in supercomputers, over the objections of the Japanese. The Germans expanded their sales of machine tools, notwithstanding U.S. opposition. As a result, it has been difficult historically to achieve agreement on a multilateral approach to controlling the various kinds of dual-use equipment and technologies that could contribute to the development of dangerous weapons.

Multilateral Cooperation

The difficulties associated with achieving arms-control agreements and putting in place effective export regimes have led to the design of another approach, known as multilateral cooperation. This approach generally focuses on preventive activities, including information sharing and crisis-management planning, and on expanding links among countries between their domestic agencies involved in law enforcement and customs, their intelligence agencies, and their foreign ministries and embassies.

The United States, Russia, and the other G-7 countries designed such an approach in response to the potential threat posed by the large amounts of nuclear fissile materials becoming available with the elimination of the vast superpower weapon stockpiles. Reports of smuggling attempts in Germany in the summer of 1994 sparked the effort. By the Moscow Summit in 1996, Russia had stopped denying the existence of the problem and agreed to a multilateral effort, the centerpiece of which was a program for preventing and combating illicit trafficking in nuclear materials. Focal points were named in each government to be responsible for gathering and evaluating information on nuclear smuggling incidents, communicating among all government agencies, and coordinating a response. International cooperation among law enforcement, intelligence, and national laboratory experts was expanded, including efforts to improve forensic analysis techniques for seized nuclear material. In this case, these steps complemented efforts to improve Russia's system for controlling nuclear exports.

More recently, the United States, Russia, and five other countries agreed to cooperate in defeating computer crime by pledging to coordinate efforts to combat industrial espionage, money laundering, and other wrongdoing in cyberspace; develop new crime-fighting techniques; and search for and prosecute high-technology criminals, even when extradition laws do not apply. (Krauss, 1997.) The key to a successful multilateral approach is a common perception of the potential threats and vulnerabilities.

INFORMATION SYSTEMS AND TECHNOLOGIES

What does this history suggest for the role that arms control, export regimes, and multilateral cooperation might play, individually or collectively, in the age of information warfare? Critical to answering this question will be how the opportunities and threats of information-warfare systems and technologies will evolve.

Arms Control

The attractiveness of arms control will depend importantly on who the potential adversaries will be and on what their goals and calculations are. If the main threat is assumed to arise from nongovern-

mental groups, or from isolated rogue countries, arms control would not be very effective, for they would not be expected to participate. But if the future threat arises, even in part, from nation-states, the possibilities for arms control need to be considered.

The United States has established maintaining superiority, or dominance, in information warfare into the 21st century as its strategic goal. Arms control in this strategy could become a potential liability, because it would be premised on the United States accepting some constraints on its information-warfare capabilities and potential military operations. Most arms-control agreements also assume that the negotiating outcome will be equal limits, not superiority for one party. Equality is often difficult to quantify, and arms control has at times resulted in advantages to one side or the other. But politically, it remains extremely difficult for another party to accept inferiority to the United States in a formal arms-control treaty.

Nevertheless, even when the United States is able to sustain a strategy of superiority, one possibility for arms control would be to ban information-warfare weapons, which the United States and other parties would view as to no one's advantage to develop and deploy. A possible candidate might be a widely discussed future weapon known as the electronic pulse system, which would be designed to attack computer-based systems.

The U.S. military can be expected to resist banning any "new" weapon system before understanding the capabilities it could provide. Potential adversaries may not be willing to give up any potential information-warfare capability. But the United States would have some leverage if it were to determine that a ban would be useful, since the United States would be willing to forgo a weapon that it could certainly be expected to produce. At the same time, the United States could not agree, until it was confident that all countries capable of making the weapons were parties to the agreement and that nongovernmental groups would not be able to acquire them.

If a ban is sought, a key issue would be the choice of an approach to verification. One would be for individual countries to make unilateral commitments that others would reciprocate. Another would be to proceed as in the case of the Biological Weapons Convention, in which the parties formally committed simply to destroy their biological weapons but without any provisions for verification. At that

time, the parties judged that no one could expect to achieve an advantage from any use of biological weapons, so relying on the self-interests of the parties to carry out their commitment was sufficient. Still another approach would be to negotiate a detailed agreement with extensive verification requirements and inspections to deter cheating and win congressional support. The problem is that such an agreement would be technically difficult and very time-consuming to negotiate.

The risk of not pursuing any arms control is that the abilities of potential adversaries to acquire information-warfare capabilities would not be constrained in any way. Over time, this could threaten the U.S. ability to maintain superiority.

If superiority is unlikely to be sustained, arms control could usefully be employed to limit the threats to the United States posed by the information-warfare capabilities of potential adversaries against both its military forces and domestic infrastructure.

One possibility would be for the United States to pursue formal measures with countries developing information-warfare capabilities, to build confidence and to reduce the risk of surprise attack and misunderstanding in a future crisis. In the past, such measures focused on reporting on the size and characteristics of military forces and equipment, as well as on different kinds of movements of military forces, including alerts. In the case of information warfare, agreements could be structured calling for exchanges about the characteristics of the various components of future systems and for notifications and observation of activities that would be necessary to prepare for an attack.

The first issue is whether governments would be prepared to share information about their systems, especially their newest systems. It will also be difficult to define precisely which activities would constitute preparations for an attack and whether they could be observed. Another issue is whether any of the governments would judge that such measures would actually build confidence and enhance their security, rather than unacceptably constraining their military capabilities and operational requirements. But more importantly, these measures presume that governments not only perceive a potential threat but also share an interest in building confidence. One could imagine such a possibility. The Russians, and perhaps even the

Chinese, could be concerned about the U.S. lead in these information-warfare capabilities. The U.S. interest would be in trying to avoid surprise or miscalculated attacks against its potentially more vulnerable domestic infrastructure.

Another possible means of building some confidence would be for the United States and others with information-warfare capabilities to provide “security assurances” with respect to the conduct of future information warfare, to reduce the risks of preemptive attacks against U.S. operational systems or the U.S. homeland. For example, governments could pledge not to be the first to attack domestic infrastructures with computer viruses, or in future wars to forgo attacks using information warfare against domestic infrastructures.

Security assurances, however, raise many problems. Such assurances could constrain the use of one’s own information-warfare systems unacceptably. Assurances will reduce the deterrent effect of such systems by suggesting that certain conditions would need to apply before they would be used. Such pledges only represent political commitments. So it is uncertain how much confidence assurances provide, given that they may or may not be carried out in times of actual crises or war. Countries with capabilities inferior to those of the United States are unlikely to perceive any advantage in forgoing at least the threat of such future attacks. Nevertheless, the United States, whose domestic infrastructure is the most vulnerable, could potentially benefit from security assurances to which all potential adversaries agree.

Arms control offers the further possibility of achieving limits on future information-warfare systems. The issue for the United States would be whether the prospect of an uncontrolled competition in information-warfare capabilities would be sufficiently dangerous as to warrant both agreeing to limits on its own systems and, more importantly, accepting equality as the legally binding outcome of the negotiations. Other parties would need to judge whether their own security would be served by gaining equal limits with the United States in return for constraints on their own capabilities. And it is not easy to predict the outcome. The parties would have to balance the fact that the United States will be able to retain, in the absence of arms control, superior military capabilities, though not necessarily the prospect of dominance, with the fact that the United States also

has serious domestic vulnerabilities, which they could exploit if their own systems were not limited.

If pursued, arms-control negotiations would confront an incredibly complex set of issues involving, for example, how to define equality or equivalence in information systems; which systems, components, and technologies would be limited; and what standard and measures of verification would be required. While it is very difficult to see the value today of pursuing any arms-control approach, a world in which information-warfare capabilities are not controlled could be very dangerous.

Export Controls

Preventing the transfer of critical components of information systems and technologies would appear to be useful, regardless of how U.S. strategy evolves or what threats may emerge. Controlling systems and technologies that have purely “military” applications, such as certain kinds of sensors, is reasonably straightforward. They could be included on the U.S. Munitions List, thereby requiring a license and approval before any sale.

If the United States alone is capable of developing such systems and technologies, unilateral controls would be sufficient. More likely, at least a few other countries will be able to acquire these capabilities. So the United States would have an interest in ensuring that these countries put in place similar controls. This could be achieved through formal restraint agreements, as in the U.S.-Japan Super-computer Agreement, or through informal understandings.

Much more difficult will be controlling the information systems and technologies (the communication technologies, computers, and software) that have both military and commercial applications. U.S. multinational corporations will wish to use such technologies in their international networks and operations, and U.S. companies will seek to market the technologies internationally. Moreover, as technologies evolve, they will also become more affordable. So, these information systems and technologies will become easily available to potential adversaries, unless they are specifically controlled by all potential manufacturers.

If the United States assumes that it can expect to maintain superiority in information warfare, through its own technological advances and management skills, preventing the dispersion of dual-use information systems and technologies would not be especially critical. If these could be used by others to challenge U.S. superiority, or if superiority is not going to be sustainable, export controls would be more important. This would be the case even if all they could be expected to accomplish would be to delay, rather than prevent, potential adversaries from acquiring certain information-warfare capabilities.

For example, the argument is made that superiority in information warfare will depend on the development of a “knowledge system” that will synthesize existing and new information systems and thereby permit the introduction of technologies into military capability more quickly than the competitors can. In this case, the dispersion of the individual information components and technologies might not be particularly risky. But keeping other countries from obtaining the means of synthesizing all of these would be very important. The issue then would arise as to whether controls could be effectively designed and implemented for the knowledge or method by which a synthesis will occur.

Putting an export-control regime in place for information systems and technologies would not be an easy task, but experience suggests that it is possible. Supercomputers and commercial encryption, which are key components of information-warfare systems, are already controlled as a means of achieving other nonproliferation goals, by the United States and other members of the Wassenaar Arrangement.

U.S. policy calls for a ban on the transfer of the most sophisticated supercomputers and technologies to all countries and prevents certain other supercomputer systems and technologies from being transferred either to nuclear-weapon-related facilities in such countries as Russia, China, and Israel, or to countries that pose a nonproliferation risk, such as India and Pakistan. Difficulties have arisen in ensuring that such controls are observed; witness the recent cases of sales to Russian and Chinese nuclear facilities. And the effectiveness of these controls can be somewhat muted by the linking of computing systems of lesser capability. But U.S. nonproliferation policies are being served by these controls.

Today, the United States also strictly controls transfers of encryption used for military purposes and limits international sales of commercial encryption above certain thresholds. The policy is extremely controversial, because the knowledge underlying these encryption technologies easily diffuses across national boundaries. And many do not share the Clinton administration's view that the dissemination of advanced encryption systems poses a threat to U.S. intelligence capabilities and law enforcement. But the controversy focuses primarily on the utility and effectiveness of the encryption policy, not the ability of the U.S. government to implement its controls, even though they are technically complex.

Designing an export-control system will raise a number of difficult issues. One would involve decisions about which information systems and technologies to control. Another would be whether effective controls require that all the critical components of an information-warfare system be covered, or only a few of the most critical.

Take the example of computer software agents (viruses) that could automatically find and destroy certain kinds of instructions in an adversary's surveillance system. Such agents would be extremely useful in U.S. military operations but would be very dangerous in the hands of terrorists or rogue states. So controlling their export would seem to be a high priority. But would it be technically feasible to control such agents? Absent such controls, would the overall export regime be effective?

Export-control regimes are attractive because their focus on individual sales ensures that governments, nongovernmental groups, and individuals are covered. So another issue that will arise is whether the controls should be global, to avoid any loopholes, or targeted on individual countries or groups, to interfere less with commercial trade.

A large number of countries will have the ability to produce and sell dual-use information systems and technologies, so a successful export-control strategy would require a multilateral approach. Gaining the support of other potential suppliers would be a real challenge. The Wassenaar Arrangement could provide a forum for assessing the character of the potential threat and its control lists could include specific information systems and technologies.

History suggests that these suppliers will continue to resist any loss of their national sovereignty and will not be prepared to coordinate their export policies, unless an extremely serious threat emerged. But if this were to occur, they might be prepared to coordinate their export-control policies by defining lists of items to be licensed, establishing rules of restraint on transfers, and committing to sharing information on their licensing decisions.

Multilateral Cooperation

Arms control and export regimes are not only constrained in the kinds of threats they can address but are also extremely difficult to design for the age of information warfare. So the United States is going to need to find other ways to ensure a credible military strategy while reducing its domestic vulnerabilities. One possibility would be to launch an effort involving multilateral cooperation with countries that face similar potential threats. The recent President's Commission on Critical Infrastructure Protection recommended a number of steps that could form the initial elements of such an effort. The commission called for

- an assessment of the characteristics of the risks of information warfare, to reach a common understanding of the potential threats
- the design of protective measures and practices to reduce the vulnerability of the information systems and networks
- the sharing of information and analysis in a timely way on the activities of potential adversaries and unusual happenings in their infrastructures, to be able to respond to potential threats
- steps to deter an attack on critical infrastructures and, should deterrence fail, to cause the attacker to cease and desist
- ways to respond to the basic needs of the populace following a disaster and to restore and reconstitute the infrastructures.²

Each country would need to tailor the specific steps to its own particular vulnerabilities. But these steps provide a good agenda for a

²President's Commission on Critical Infrastructure Protection (1997).

multilateral approach that would prepare for joint actions to respond to the threats if they materialize in the future.

A STRATEGY DURING THIS TIME OF UNCERTAINTY

Too many uncertainties exist today to be able to decide definitively what role, if any, arms control, export regimes, and multilateral cooperation will play in the age of information warfare. The United States needs, nevertheless, to set the stage for these decisions by taking steps now to reduce the uncertainties, achieve basic understandings about its strategic assumptions, and ensure that, as the systems and technologies are developed, they do not produce instabilities or vulnerabilities.

The first task involves intelligence and analysis. The United States needs to understand more precisely the characteristics and capabilities of future information-warfare systems and the technologies and management skills that will be critical to their development. This would provide a basis for determining who will be able to develop information-warfare systems: only a few governments with an advanced technological base and managerial skills, or any dedicated group anywhere in the world. Under what circumstances and in what time frame will others achieve information-warfare capabilities?

The second task should be for the United States to come to basic understandings about its strategic goals and assumptions with respect to information warfare. What will the characteristics of the threats be? What will U.S. operational military requirements and vulnerabilities in the age of information warfare be? Is superiority a sustainable strategy for the long term? Could the United States be sufficiently confident in the future to base its security on the existence of information-warfare superiority? What risks can be expected to arise for American society?

The United States has an interest in ensuring that the development of information-warfare systems does not lead to global instabilities. So the third task should be for the United States to take steps to ensure that other countries understand U.S. goals and the characteristics of the information-warfare systems that it is developing. Confidence could best be built by early and extensive sharing of infor-

mation. Engaging the Russians will be particularly important, so that they do not view U.S. programs as a threat to them. This could be done bilaterally or within the framework of exchanges between NATO and Russia. In return, the United States would gain greater understanding of the plans and capabilities of others. Such discussions could also set the stage for more-formal arms-control negotiations and measures, if such a decision is taken in the future.

Export regimes would appear to have a role in preventing the transfer of certain information systems and technologies, irrespective of the specific ways in which the threats will emerge. So the fourth task should be to address how the systems and technologies might be controlled effectively as they are being developed. Among the basic questions that will need to be answered are the following: What critical components in information-warfare systems would need to be controlled: systems, technologies, or management expertise? Can any or all of these be controlled effectively? If so, what is the prospect that the controls would successfully prevent, or at least significantly delay, the development of information-warfare systems by others?

Answering these questions will require cooperation within the United States between the military, which is developing the actual systems; the companies that will be producing and marketing them; and the government officials who will be responsible for their licensing. As success will require support from other countries that will be developing information-warfare systems and technologies, informal discussions focused on these same questions should begin soon.

While the future evolution of information technologies is uncertain, the potential risks to the United States are clear. So the final task should be for the United States to begin to work with other friends and allies to find ways to cooperate in preventing potential threats to their domestic infrastructures.

Carrying out these tasks will prepare the United States for the possibility that arms control, export regimes, and multilateral cooperation will have an important, perhaps even critical, role to play in promoting global peace and stability in the age of information warfare, as they have done in the past.

REFERENCES

Krauss, Clifford, "8 Countries Join in an Effort to Catch Computer Criminals," *New York Times*, December 11, 1997, p. A12.

President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, October 1997.