THE EMERGING GLOBAL INFORMATION INFRASTRUCTURE AND NATIONAL SECURITY

GREG RATTRAY

The United States has encouraged other nations to follow its lead toward a new telecommunications era by building accessible, open National Information Infrastructures (NIIs). The concept of a Global Information Infrastructure (GII), outlined by U.S. Vice President Gore to the International Telecommunication Union (ITU) on March 21, 1994, focuses on an interconnected global telecommunication highway paved with gold and good intentions. Other nations have proposed similar GII plans and ideas. However, there is a growing realization that this information age will also have a dramatic impact on security affairs. The success of new technologies during the Gulf War, as well as the effects of hackers and information systems failures on air traffic control, the banking system and the U.S. Department of Defense (DOD), indicates that a new type of national security threat is emerging: nations' reliance on information technology and information networks could be exploited by a variety of actors for strategic attacks.[1] Nations must find ways to capture the benefits of global telecommunications networks while limiting their vulnerability.

Information infrastructures consist of networks of computer hardware and software, data storage and generating equipment, abstract information and its applications, trained personnel and interconnections between all these components. The infrastructure includes the public-switched telephone network, satellite and wireless networks, private networks and the Internet and other computer and data networks.[2] GII development would be based on the principles of private investment, competition, flexible regulatory frameworks, open access to network providers and universal service.

While nations have developed their own information infrastructure goals and strategies based on the U.S. principles, most see NIIs as linked in an in-

Greg Rattray is a major in the U.S. Air Force and a doctoral candidate at the Fletcher School of Law and Diplomacy. His previous assignments include assistant professor of political science at the U.S. Air Force Academy, where he was deputy director of the USAF Institute for National Security Studies.

terconnected, interdependent global system. Higher levels of interdependence between individuals, organizations and states through information infrastructures will likely involve increased vulnerability to disruption and attack. However, this prospect is largely an afterthought to those painting the GII picture.[3] Neither individual nations nor international organizations, such as the ITU, international satellite operators or trade organizations, have adequately addressed national security concerns emerging from the creation of a GII.

A New Means for Confronting the United States

The United States will likely continue to dominate conventional battlefields for the foreseeable future. In their Spring 1996 *Foreign Affairs* article, Joseph Nye and William Owens argue the U.S. "advantage stems from Cold War investment and America's open society, thanks to which it dominates important communications and information processing technologies—space-based surveillance, direct broadcasting, high-speed computers—and has an unparalleled ability to integrate complex information systems."[4] Other countries are aware of these strengths and fearful of the United States's willingness to employ such capabilities.[5] However, increased dependence on information technology in the United States makes our information infrastructures high-profile targets for efforts to influence U.S. policy. In 1991, the National Research Council began to document the large scale vulnerabilities of a U.S. society dependent on computer-based information processing systems in a study entitled *Computers at Risk.* A 1993 study by those responsible for the National Communications Systems concluded, "The threat that contemporary computer intruders pose to the public switched network is rapidly changing and significant."[6] A 1996 U.S. Government Accounting Office study entitled "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" concludes that "the hundreds of thousand of attacks that the Defense has already experienced demonstrate that (1) significant damage can be incurred by attackers and (2) attacks pose serious risks to national security."[7]

U.S. Reliance on Information Infrastructures

Vice President Gore describes the U.S. NII as consisting of "hundreds of different networks, run by different companies and using different technologies, all connected together in a giant network of networks."[8] Among the largest and most complex of these networks are those operated by the DOD. The security of defense-related telecommunications and information networks has long been a concern of the U.S. military, and the Defense Information Infrastructure (DII) is heavily connected to both the GII and NII. Today, over 95 percent of U.S. military communications travel over commercially operated networks.[9] The military relies on international commercial information networks to provide command, control and intelligence to U.S. forces in operations such as the NATO peacekeeping efforts in Bosnia.

Information systems are crucial to the operation of other key government

institutions including the Federal Reserve System, Federal Bureau of Investigation, Justice Department, Federal Aviation Administration, U.S. Postal Service, Social Security System and the Internal Revenue Service. The Federal Reserve System uses FEDWIRE electronic networks to transfer funds between branches. FAA radar systems have demonstrated their frailty in numerous cases, causing major disruptions in air traffic and threatening a major catastrophe. Provision of many public utilities and emergency services are also highly dependent on information systems. Most public utilities providing services such as natural gas, water and sewage treatment are highly dependent on computer-based control systems which are vulnerable to intrusion and disruption.[10] In turn, these information systems and infrastructures rely in varying degrees on the electric power system, which can also be disrupted through information attacks and sabotage. The timing systems of telecommunications and computer networks are also crucial to their functioning and could be disrupted. Phone network and "911" services can and have been disrupted by outside intrusion on numerous occasions.[11]

Command and control systems can be bombed, telecommunications cables cut, microwave antennas broken and computers smashed or simply turned off.

The commercial sector's reliance on information infrastructures grows every day. An average of $1 trillion is transferred among U.S. banks daily and $800 billion is transferred among partners in international currency markets every day.[12] The distribution of goods and services based on just-in-time inventory and delivery are highly dependent on advanced information networks. The vast majority of the transactions and information flows described above rely on the vulnerable public switched network for transmission by landline, microwave or satellite means. According to the Council on Economic Advisors, the combined telecommunications and information technology sectors of our economy represent 9 percent of U.S. GDP, a figure which could double in the next 10 years.[13]

Susceptibility to Disruption

The susceptibility of information infrastructures to disruption and exploitation by both outsiders and insiders is increasingly clear. The ability of hackers to get into DOD computer systems has been well established, most recently by the U.S. Attorney General's March 1996 indictment of an Argentine hacker who used access to the Harvard University network to achieve further access to DOD, Navy and NASA computers.[14] Even more telling is a series of "red team" tests run by the Defense Information Systems Agency (DISA) in 1994 to evaluate defense information infrastructures. DISA tested nearly 9,000 DOD computers networks with simple "front-door" attacks and managed to gain control of 88 percent of these networks. Only 4 percent of these networks

recognized they had lost control and only 0.2 percent of the networks reported being attacked.[15]

While the relative vulnerability of other governmental, public service and commercial information systems is not known, the banking system is known to have sustained large losses from credit card fraud. The telephone networks have also undergone numerous large-scale failures, such as the nation-wide collapse of the AT&T system on January 15, 1990, resulting in 70 million uncompleted calls. The impact of malicious software, generally known as "viruses," has also caused major disruptions, such as the Internet Worm unleashed by Robert Morris in 1988 that shut down Internet services for several days. Citicorp has admitted that a Russian hacker managed to siphon electronically $12 million in 1995.[16] More recently, the *London Times* reported that financial institutions in London have made extortion payments of hundreds of millions of dollars to "cyberterrorists" who threatened to disrupt their operations.[17]

Attacking Information Infrastructures

Information systems and networks have long been targeted by mechanical methods of disruption and destruction during war and peace. Command and control systems can be bombed, telecommunications cables cut, microwave antennas broken and computers smashed or simply turned off. The electronic components and transmissions of information systems and networks are also vulnerable to disruption and damage from electro-magnetic energy directed at them. In the military realm, efforts to jam transmissions have occurred since radios began to be used in World War I.[18] During the Cold War, those concerned with guaranteeing U.S. nuclear command and control communications under an attack paid considerable attention to the problem of the electro-magnetic pulse generated by nuclear detonations. Recently, some analysts have highlighted the possibility of generating such effects in a much more localized and directed form.[19] To the extent that adversaries can gain and maintain sufficient proximity to key information systems, they may be able to use directed energy attacks as part of their offensive plan.

Most of the attention surrounding the possibility of strategic information attacks has dealt with threats from electronic intrusion and disruption of the computer systems that underpin much of our information infrastructures. The Office of Technology Assessment has categorized threats down into two types: crackers and other intruders, and viruses and other malicious software. The intent of attacks can range from total paralysis to intermittent shutdowns, random data errors, wholesale theft of information, theft of services, illicit systems monitoring, injection of false information and information-based blackmail.[20] A number of studies have discussed creating corrupted hardware platforms or systems components which could be inserted into an adversary's information systems and allow the attacker access to monitor, disrupt or destroy an adversary's system.

An information attack's effectiveness can be enhanced through the presence of insiders. The significant threat presented by disillusioned employees and others with sanctioned access is a recurring theme in the information

security literature. Insider access can be critical in providing information on network access, operations and vulnerabilities; conducting a physical attack (such as shutting off the power) in conjunction with electronic attacks; or inserting malicious software and/or hardware. To the extent potential adversaries can co-opt individuals with access to key information infrastructures, their ability to conduct strategic information attacks may be greatly enhanced.

To make matters worse, the tools to attack information infrastructures are cheap. A recent RAND report states:

> Unlike traditional weapons technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.[21]

Software tools necessary for electronic attacks, such as the Systems Analysis Tool for Network Administrators (SATAN), can be easily and anonymously downloaded from numerous Internet File Transfer Protocol (FTP) sites.[22] The primary technological challenge for potential adversaries is less the acquisition of hardware and software described than the knowledge of how to use the tools. As a result of widely available means, a variety of state and nonstate actors (such as terrorist and organized criminal groups) who see themselves as potential U.S. adversaries will likely endeavor to build the capability to conduct information attacks.[23] The growth and intended open access to the GII gives will permit U.S. adversaries worldwide very quick, unimpeded access to attack these key infrastructures at vulnerable points. The Internet, in particular, has historically been a source of information infrastructure.

Growing National Security Concern about Information Infrastructure Vulnerabilities

The vulnerability of our information infrastructures has become a matter of the highest level of policy-making concern. A series of articles in the summer of 1995 culminated in a *Washington Post* article that discussed the vulnerability of the U.S. information infrastructure as a potential "electronic Pearl Harbor."[24] Congress has entered the picture by adding an amendment to the 1996 Defense Appropriations Bill, requiring the President to submit an explanation of national policy for dealing with potential NII attacks.[25] This concern culminated in July 1996 with an Executive Order establishing a Commission on the Protection of Critical Infrastructures. The Commission will "assess the scope and nature of vulnerabilities of, and threats to, critical infrastructures" including telecommunications, electrical power system, gas and oil storage and transportation, banking and finance, transportation, water supply systems and continuity of government.

The United States's increasing reliance on information infrastructures and the intermingling of defense and other portions of the NII with the GII have increasingly put crucial military and economic outside control of those responsible for national security. While the DOD and associated agencies can

exert varying levels of control over government information networks, no mandate exists to protect such potentially vulnerable networks in the public service or commercial sectors. Increasing levels of connectivity with an open-access GII may exacerbate the degree of vulnerability. Yet, the recognition of a potential new national security threat has apparently not crossed the bureaucratic boundaries to those responsible for NII and GII development. As of January 1997, the Commission on the Protection of Critical Infrastructures still lacked adequate participation from the civilian sector. GII advocates within and outside government have strongly argued the case regarding the negative impact of government and regulatory agencies' involvement on network efficiency and raised concerns about the protection of personal privacy.

Those responsible for national security should assume they no longer have a trump card in determining telecommunications and information infrastructure policy.

Those responsible for national security should assume they no longer have a trump card in determining telecommunications and information infrastructure policy. The 1984 divestiture of AT&T's Bell Operating Companies, which took place despite the strenuous objections of Secretary of Defense Caspar Weinberger, began an era where the national security community must learn to deal with defending a country driven by the economic imperatives of information.[26] As awareness of potential national security vulnerabilities stemming from disruption of the DII and NII grows, the time is ripe for examining how past approaches to controlling technologically-based threats may be applied to the emerging GII.

Learning Lessons from Past Efforts to Control Technologies

Since World War II, the United States has pursued two primary approaches to deal with the consequences of threatening technologies: the use of export controls to prevent the spread of the technologies and arms control efforts to deal with both the spread and consequences of possession of threatening technologies. The steps taken can be unilateral, bilateral, multilateral or strive for global compliance. Nations can learn lessons from these past approaches to assess and limit the vulnerabilities of information infrastructures while attaining the economic benefits, democratic discourse and improved public services which result from the GII. While this section divides export control and arms control for purposes of analysis, the United States has generally pursued the two approaches in tandem.

The problems of securing the GII are clearly different than past security challenges and should be examined from a variety of perspectives. Other an-

alytical approaches should also be explored based on past efforts to deal with transnational crime and drug smuggling. Some analysts have suggested looking at the Center for Disease Control and the World Health Organization as potential models for treating pathologies inherent in the Internet.[27] The cumulative impact of multiple approaches can only be positive. Using export controls and arms control as possible models provides one point of departure for new ways of thinking about these new issues.

Export Controls

The United States has long used export controls to address the potential transfer of dual-use technologies to potential adversaries. During the Cold War, the primary focus was on the strategic competition with the Soviet Union. As the leader in a broad range of technologies, the United States instituted a system of unilateral export controls in 1949, as well as an international effort through the Coordinating Committee on Multilateral Export Controls (COCOM). Although export controls may have slowed the Soviet bloc's development of highly advanced electronic/sensor systems and high-performance computers, export controls also resulted in commercial losses for U.S. firms, considerable leakage and a potential incentive for adversaries to boost indigenous technology development. As the Cold War waned, the number and technological scope of restricted items was reduced. In the spring of 1993, COCOM was disbanded as the government endeavored to transform its relationship with its former adversaries into one of economic cooperation and partnership.

In the late 1970s and into the 1980s, the United States also became increasingly concerned with the nonproliferation of weapons of mass destruction. The initial focus was on nuclear weapons and enforcing the provisions of the Nuclear Non-Proliferation Treaty. The 1980s saw growing concern with other types of dual-use technology transfer in the areas of ballistic missiles and chemical/biological weapons. International technology control regimes as well as arms control efforts were instituted in these areas to help control the transfer of "threatening" technologies. While some successes in combating proliferation occurred, assessments of multilateral export control regimes demonstrate an increasingly pessimistic view of the ability to control the transfer of these technologies. Even in the case of nuclear technology, where technologies and related facilities were of limited dual-use, expensive, complex, and relatively observable, the ability of Iraq to circumvent the IAEA controls in pursuing nuclear weapons has raised a cautionary note.[28]

The ability of Iraq to circumvent the IAEA controls in pursuing nuclear weapons has raised a cautionary note.

In general, as the degree of dual-use for a given item or technology increases, the ability of export control regimes to inhibit technology diffusion decreases.[29] The President's assistant for science and technology, John Gibbons,

recently wrote, "High technologies are increasingly difficult to control, owing to advances in global scientific literacy and the world-wide mobility of people and information." The characteristics of information technology generally, and those of the technological tools necessary for strategic information attacks particularly, are characterized by the trends limiting export control effectiveness. In examining U.S. export control of computer technologies to the former Soviet Union, Seymour Goodman concludes:

> Technological advance and changing geopolitical relationships have increased the availability of mass produced Western technologies. It has become difficult for export controls to prevent or significantly slow the flow of products like powerful microprocessors or scientific workstations that are made in large numbers. It is becoming increasingly possible to build parallel processors using commercial technologies.[30]

Encryption as a Case Study

The difficulties of controlling software-based technologies such as those necessary for strategic information attacks can be illuminated by examining U.S. efforts to control encryption technology. Until recently, military and intelligence organizations had a virtual monopoly on the development of sophisticated encryption algorithms. During the Cold War, significant efforts were made to regulate the private sector development of encryption technologies and control any efforts to export the algorithms, software and hardware involved. Strong encryption technology is still considered a military-related export and is controlled by the State Department with the advice of the National Security Agency. Yet, as the private sector's sophistication with using telecommunications networks increases, tensions have grown. The need for personal privacy and self-protection of communications conflicts with national security and law enforcement desires to monitor criminal activity at home and collect intelligence abroad.[31] U.S. hardware and software producers concerned about increasing consumer demand for the security provided by encryption are worried that current U.S. export controls will hurt their international business. In fact, an increasing number of analysts advocate making encryption widely available to the public to reduce the vulnerability of our public and commercial information infrastructure to outside monitoring and intrusion.[32]

The U.S. government continues to resist export of strong encryption, yet expertise in cryptography has expanded internationally and the technologies and products are widely available outside the country. A recent study concludes "Encryption products are produced in 35 countries worldwide. The U.S. is no longer the sole source of information security—of 1,035 encryption products produced world-wide, 435 are produced outside the United States."[33] As with other software tools for protection of information infrastructures, encryption algorithms and software are freely distributed through the Inter-

net. No international agreement exists regarding the proper approach to control encryption technologies. The Scandinavian countries believe widespread use of encryption provides increased personal privacy. In Japan, the ability to produce and export strong encryption is seen as a source of potential comparative advantage for their commercial sector. Japanese companies have aggressively pursued the development and sale of products with encryption capabilities.[34] Recent evaluations suggest current U.S. policy is unrealistic regarding its ability to constrain world development and use of strong encryption technology, and potentially harmful to its own information technology producers. In general, export controls have limited utility in constraining actors abilities to conduct strategic information attacks.

Arms Control and Securing the GII

Another means to manage the consequences of potential adversaries having the technological capability to threaten national security is through arms control. The imperative for arms control springs from the existence of a security dilemma in a global system where states and other actors have the ability to build or acquire capabilities to harm others. Trust often does not exist between these actors. Therefore, actors interpret incoming information on the military capabilities of rivals in the worst possible light. An upward spiral, or arms race, can ensue as each actor tries to avoid a situation of military disadvantage. Additionally, an arms race increases political tension between states, raising the possibility and severity of crises and possibly causing war. Arms control tries to address the negative effects of the security dilemma. It has been defined as "a process involving declared steps by a state to achieve security through cooperation with other states. This cooperation can be unilateral, bilateral or multilateral."[35] While the tools used for strategic information attacks are generally not referred to as arms, they can certainly be viewed as creating potential security dilemmas between states and other actors. These new "arms" are very difficult to observe and the growing literature about their potential for disruption already indicates a propensity for worst-case analysis. Also, while the concept of the security dilemma was developed in reference to state security, the analysis in this article extends the concept to deal with nonstate actors. Even though such actors are less transparent in terms of their intent and activities, states have long tried to deal with security challenges posed by terrorists and other transnational groups. If nonstate actors begin to use the GII for strategic information attacks, efforts to "control" the means for these attacks will need to deal with such adversaries.

If nonstate actors begin to use the GII for strategic information attacks, efforts to "control" the means for these attacks will need to deal with such adversaries.

During the Cold War, arms control efforts generally focused on lengthy, formal negotiations to manage the strategic balance between the superpowers.[36] Given the dire consequences of a superpower nuclear exchange or a major conventional war in Europe, the primary objective of arms control during this period was to avoid war through crisis stability. The goal was to reduce each sides' incentive to launch a surprise attack and to reinforce the concept of mutually assured deterrence.[37] Of secondary importance was stabilizing both the nuclear and conventional arms races in order to minimize the cost of war preparation. Because of the importance of the strategic balance to both superpowers, strict verification of adherence was required. The United States was particularly concerned with verification given the relative difficulty of monitoring Soviet forces and weapons programs.

Distinguishing These Efforts from Securing the GII

A fundamental difference between the arms control approaches outlined above and efforts to limit strategic information attacks relates to the actual nature of the weapons involved and the ability to verify whether the other side is properly following the terms of the agreement. Cold War arms control approaches stressed managing the types and numbers of weapons systems possessed by each superpower or bloc. The items were large and observable: strategic missile systems, submarines, aircraft and tanks. The presence and destruction of these systems were verified by large and expensive intelligence organizations through technical means of collection (particularly satellite imagery) and on-site inspections. These means were felt to be capable of deterring all but marginal, militarily insignificant cheating due to the observability of the systems and long-standing intelligence procedures for tracking the items subject to control. In 1990, the Congressional Budget Office estimated that the one-time cost of implementing the START I agreement would be between approximately $1.2 billion followed by annual cost of approximately $250 million.[38]

Regimes built around observable, tightly monitored objects will not work in controlling the tools necessary for strategic information attacks.

Regimes built around highly observable, tightly monitored objects will not work in controlling the tools necessary for strategic information attacks. The technological tools necessary for damaging information infrastructures won't be observable and even if massive on-site inspection procedures were implemented, the ubiquity of computer processing capabilities today and the ease of transmitting and hiding electronic tools would make discovering their existence near impossible. Trying to construct agreements that specify "force"

levels in dealing with tools for strategic information attacks would prove as futile as export controls.

The Cold War efforts took place between governments and were bilateral in the sense of being between superpowers or alliances. Efforts to cooperatively secure the GII have to involve a large number of parties, including intergovernmental organizations and the private sector. While technologies underlying the weapons of the Cold War were developed by governments, the technologies involved in information infrastructure attacks are now globally diffused in the commercial sector. However, there may be some lessons to learn from the Conventional Forces in Europe (CFE) process in understanding the challenges of bringing an agreement together among allies (such as NATO) first before opening discussions to a wider audience. At least one U.S. CFE negotiator has commented that the intra-alliance process of defining and trading equities among the 16 NATO nations proved much more difficult than reaching agreement with the Warsaw Pact at numerous times during the negotiation.

Arms control dialogues during the Cold War set important precedents for international security cooperation that could prove useful for securing the GII. Providing an open international forum for claims and opportunities for parties to share their perspectives on issues did not entirely alleviate the threat of war. However, the parties realized the value of cooperation and confidence-building measures that could be reinforced through verification attempts. Understanding how other actors conceptualize these new threats to national security will be a crucial first step in controlling their effects.

The Multilateral/Global Arms Control Approach

Efforts to limit the spread and use of nuclear, chemical and biological weapons, collectively known as weapons of mass destruction (WMD), have to deal with the challenges of dual-use technologies as will clearly be the case with information attack technology. The WMD regimes are aimed at limiting the global diffusion of potentially harmful technology while generally allowing peaceful uses. In doing so, these regimes all strive for universal adherence to treaties among states. In the words of one author, such arms control is "arms control for everyone."[39] Multilateral efforts to control WMD existed during the Cold War but the level of international attention concerning the proliferation of WMD rose dramatically after the demise of the Soviet Union and the Persian Gulf War. With decreased superpower competition reducing the dangers of surprise nuclear attacks and need for costly arms races, arms control efforts focused on achieving transparency and sharing information on the diffusion of WMD technologies.

Distinguishing These Efforts from Securing the GII

Nonproliferation regimes still focus on controlling physical precursors in the weapons creation process. The size and complexity of the technologies vary, but they are still tangible. As a result, these regimes continue to stress

on-site inspection regimes. The substances used in biological weapons may most closely parallel the nature of the tools for strategic information attack. Hospital and research labs must have small quantities of deadly viruses to conduct disease research. Yet, these small amounts can be rapidly grown into large quantities for use in weapons.[40] This situation is analogous to the need of network systems administrators to have tools such as SATAN to identify their own vulnerabilities, but can also be used to identify weaknesses of other computer networks. Electronic tools can also be easily replicated and dispersed. However, biological weapons must be put into a deliverable form and physically transported to the target, creating another layer of observability, especially in dealing with toxic materials.[41] The electronically transferable tools for disrupting information infrastructures make them nearly impossible to observe. A person carrying a disk in his or her pocket may well be equipped with a "weapon" capable of global reach when the disk is put into a computer with a modem. A treaty that tried to list prohibited types of malicious software tools might be envisioned similar to the categories of chemicals in the CWC. However, the ease of modifying electronically-based information in a way which would put the new creation outside of a controlled list makes such a concept clearly unworkable.[42]

A person carrying a disk in a pocket may be equipped with a "weapon" capable of global reach when the disk is put into a computer with a modem.

Also, part of the effectiveness of the WMD regimes revolves around outlawing weapons with clearly abhorrent effects.[43] Unfortunately, the world has seen the effects of WMD use with the atomic bombs dropped on Hiroshima and Nagasaki, the 1979 anthrax outbreak at a Soviet biological weapons research and development facility and the use of chemical weapons in the Iran - Iraq war. A sense of moral outrage will likely never exist regarding tools for strategic information infrastructure attacks. Their impact may be simply disruptive, and as of today we have no clear examples of their widespread use in a structured attack.

A fundamental lesson of efforts to control the proliferation of WMD is that while the treaties do not create 100 percent compliance, their existence is crucial to the creation of international norms for dealing with discovered violators who misuse diffused, dual-use technologies.[44] In making the case for U.S. Senate ratification of the CWC, Michael Modie, President of the Chemical and Biological Weapons Arms Control Institute, recognizes that for such technologies, arms control can not focus on overly strict constraints. Potential proliferators have the ability to acquire means to make these weapons. He argues that a single violation is less critical to global peace or a nation's security than the arms control efforts of the Cold War. Rather, the goal of such regimes is to raise the chance of detection and deter actors from choosing to acquire these

capabilities.[45] Simply becoming a hold-out state from a treaty such as the NPT, CWC and BWC creates suspicion, causing states and other actors concerned to focus their intelligence efforts on the holdout. North Korea's recalcitrance in signing the NPT and subsequent delay in coming to an inspection agreement with the IAEA made it an important target of U.S. intelligence efforts. In conjunction with the IAEA, the U.S. raised the issue of possible North Korean nuclear proliferation to the highest levels of international concern in the summer of 1994, before coming to an agreement setting up a system of rigorous inspections in September of that year.[46] Formal conventions provide a critical legal and moral basis to deal with technologies which cannot be completely controlled. Creating the conditions for deterrence and retaliatory actions against strategic information attacks may prove a central rationale for cooperative security efforts regarding the GII.

The need to deal with nonstate actors and individuals has also become an increasingly important part of the WMD regimes.

Other important lessons can be learned from the process of putting together and managing these regimes. The need for industry involvement in controlling dual-use technologies has been clearly recognized. In the CWC case, major chemical manufacturers, recognizing the impact the CWC would have on their industry, were able to devote resources and personnel toward helping design the terms of the accord. Part of their plan was to secure an international agreement that would obviate the need for many of the burdensome licensing and export restrictions which had been applied over the years by Congress and the executive branch.[47]

The recent efforts to examine possibilities of adding a verification protocol have included extensive discussions with the biotechnology industry concerned with loss of commercial proprietary information.[48] Any efforts to control and monitor the spread of technologies and capabilities threatening to the GII would require substantial private sector involvement given the leadership role the private sector is assumed to have in constructing and governing the GII.

The need to deal with nonstate actors and individuals has also become an increasingly important part of the WMD regimes. A key strength of the CWC is the provision that signatories enact legislation making treaty-violating activity a criminal offense.[49] In analyzing efforts to combat the smuggling of nuclear material, Guy Roberts notes that the lack of such laws has proved a major weakness.[50] Dealing with nonstate actors will prove crucial in securing the GII given the difficulties in distinguishing between types of harmful activities and the difficulty of securing international prosecution of known individuals and groups involved with disruptive computer network intrusions. Strong advocates of the WMD arms control regimes recognize the need for effective intelligence gathering about potential violators, defense programs to protect against the use of biological and chemical weapons, and retention of

capabilities to respond and deter such uses.[51] Establishing a GII robust enough to deal with the presence of actors who have and use the capability to conduct strategic information attacks should be acknowledged as a necessary part of any regime designed to foster security on the GII. However, efforts to deal with regime noncompliance run the risk of going too far and re-energizing the security dilemma. The 1993 U.S. DOD counterproliferation initiative focused on how the United States should respond to cases of unsuccessful efforts to stop proliferation.[52] However, other states have accused the United States of creating a rationale for preemptive attacks and a status quo protecting U.S. nuclear dominance. As a result, defensive measures to deal with arms control regime limitations must strike a delicate balance. Many nations have called on the nuclear weapons states under the NPT to provide "no first use pledges" as intermediate steps towards a more equitable regime. Given U.S. leadership in the technologies relevant to the conduct of strategic information attacks, the international community will be particularly leery of arrangements that seem to serve primarily U.S. interests.

The United States must lead the way in mitigating fears of an information arms race.

In total, the arms control experience provides an extremely useful basis for analyzing how parties involved with developing the GII may begin to deal with the questions arising from potential national security threats that are created by a globally intertwined information society.

Cooperatively Enhancing Security While Pursuing a GII

As part of the shift into the information age, leaders championing economic efficiency and libertarian causes must recognize the continuing relevance of national security concerns. At the same time, concepts of national security must move from tightly controlling threatening technologies to a more appropriate focus on dealing with the inevitable possession of capability for strategic information attacks. The first need is to build awareness of potential GII risks while building resistance and immunity of information infrastructures to attack. The Gore initiative called on nations to create a dialogue and cooperate in pursuit of his five principles. The same approach should guide efforts on the national security aspect of GII. U.S. leadership will prove central to the creation of a concerned community of states, organizations and private sector actors ready to deal with this new challenge. The global, transnational nature of emerging information infrastructures requires that the United States take a similar perspective on achieving security in this area. The United States should undertake a number of unilateral, bilateral and multilateral initiatives to create the foundation for a global dialogue on securing the GII. Unilateral initiatives should include the following:

1. Aggressively highlight information technology's role in past cooperative international security arrangements, from the 1963 Hot Line agreement between the United States and the Soviet Union, through the use of national technical means to monitor the critical strategic nuclear arms agreements such as SALT, INF and START to the availability of satellite uplinks that allowed arms inspectors in Iraq to be observed by an international audience as they were detained, leading to their release and the delivery of crucial data on Iraqi nuclear programs.

2. Make a "No First Use" pledge regarding the conduct of strategic information attacks. The United States should not renounce the capability to develop such capabilities as a deterrent capability to respond in kind. However, a "No First Use" declaration would be a crucial confidence-building step regarding U.S. intentions in the area of strategic information attacks. Other nations, such as Russia,[53] clearly see the United States as the leading power capable of making strides in this area. The United States must lead the way in mitigating fears of an information arms race.

3. Vice President Gore should publicly call for the addition of a "securing the GII" principle to the existing five GII principles as part of the next appropriate ITU forum. This announcement would establish the U.S. intent to aggressively put the issue on the international agenda.

Bilateral and multilateral initiatives should focus on dealing with strategic information attacks through existing cooperative security arrangements, particularly with NATO and Japan. The United States should not undermine its other cooperative security arrangements while dealing with GII security. Prior consultations will convince allies that their security concerns remain central to the United States and allow creation of a consensus before raising the issue with other nations. Additionally, the United States should take the global initiative and make managing national security concerns an active part of the GII process. Steps should include the following:

1. Create forums for the discussion of security concerns about strategic information attacks within the myriad of GII working groups including national governments, intergovernmental organizations and private sector stakeholders as an extension of the U.S. model outlined above. Forums should enable the exchange of information on threat perceptions and defensive measures (such as multilevel security within networks); discuss the characteristics of regulatory structure which assist and impede dealing with security concerns and address through the WTO, ITU and ISO issues such as harmonization of encryption control, monitoring, user identification and nonrepudiation.

2. Consider creating an international agency with the technical expertise to assist states and other GII users in cases of strategic information attacks. A computer emergency response team (CERT) based on the model of the U.S. CERT based at Carnegie-Mellon University could provide immediate assistance in minimizing information system disruption and damage while identifying the source of the problem. The mandate of such an agency should include security assistance programs for member states or organizations desiring help with an internal proliferation of dangerous software and hardware tools for information infrastructure disruption on a long-term basis. A country like Russia with significant economic and social challenges and an organized criminal element known to be using sophisticated electronic intrusion techniques would be a prime candidate for such assistance.[54] The U.S. Cooperative Threat Reduction Program might provide an initial model for establishing such assistance.

3. Add the security of the GII to the agenda of U.N. Conference on Disarmament. In 1994, the U.N. General Assembly passed a broad resolution on the role of science and technology in the context of international security and disarmament that "invites Member states to widen multilateral dialogue, seeking universal norms and guidelines that would regulate international transfers of high technology with military applications" which could be used as the basis for such an initiative.[55] An *ad hoc* committee within the Conference could be set up to consider the definition of a strategic infomation attack and conventions for cooperation in dealing with transnational infrastructure disruption.

Over the longer term, the Conference on Disarmament should discuss a treaty requiring all states to make strategic information attack an outlawed activity. Given the past experience with the CWC and BWC treaties and the need for industry involvement, the process for creating such an agreement should involve nongovernmental stakeholders involved with the GII. Provisions should include creation of an official body to adjudicate disputes, implement and harmonize domestic criminal laws and sanctions for non-signatories (such as prohibiting assistance for developing information infrastructures).

4. Finally, the U.N. General Assembly should discuss the formation of a transnational institution to monitor the threat to the GII and NIIs, similar to the IAEA. At the simplest level, the organization could help monitor hackers' publications and the Internet to identify potential threats and sources of prohibited activity. More extensively, an agreement could require signatories to provide data on infrastructure disruption incidents by both government and pri-

vate sector organizations to help characterize the nature and extent of the strategic information attack threat.

Conclusion

A potentially dangerous situation exists regarding the emerging GII. While the benefits from an interconnected global information society are numerous, vulnerabilities to information infrastructures have been created that threaten the well-being and security of states and societies. Existing international mechanisms and laws do not satisfactorily deal with this problem, nor do they create enforceable norms of behavior regarding use or disruption of the GII. Security problems arising from implementation of the GII principles could become significant if not properly managed by those responsible for creating, using and regulating the GII. Techniques developed from past efforts to control threatening technologies will have limited effectiveness due to the dual-use and nonstate dimensions of this new security challenge. More recent efforts to control threats such as nuclear materials and chemical and biological weapons provide important lessons regarding increasing transparency through dialogue, discovering and deterring cheating and establishing international norms and mechanisms to enforce them. This article suggests a range of initiatives to create a new dialogue and mechanisms to help attenuate, but not solve, the problem of security threats arising from the GII. Striving for a cooperative approach will demand both self-reflection by U.S. policymakers and a determination that benefits of cooperation exceed striving for competitive military. Further addressing this issue also requires the United States to exercise international leadership and demonstrate a willingness to spend political capital to achieve a more robust, usable GII.

Notes

1. See U.S. Congress, Office of Technology Assessment, "Information Security and Privacy Network Environments" (Washington, D.C.: Government Printing Office, 1994).
2. Ibid., 41.
3. In the European Agenda for Cooperation, intellectual property rights, network security and reliability are mentioned; however, new threats emerging from the GII are not addressed.
4. Joseph Nye and William Owens, "America's Information Edge," *Foreign Affairs*, Vol. 75 no. 2 (March-April 1996): 20.
5. Eliot Cohen, "A Revolution in Warfare," *Foreign Affairs*, Vol. 75 no. 2 (March/April 1996): 37-54.
6. Richard Power, "Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare," Report by Computer Security Institute (1995).
7. Roger C. Molander, Andrew S. Riddle and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Washington, DC: RAND National Defense Research Institute, 1996).
8. Al Gore, Speech to the ITU Development Conference, Buenos Aires, Argentina, 21 March 1994.

9. Seymour Goodman, "The Information Technologies and Defense: A Demand-Pull Assessment," Center for International Security and Arms Control, Stanford University, (February 1996): 6.
10. General information about such systems can be found at http://www.iinet.netau/~ianw/primer.html.
11. Fredrick Cohen, *Protection and Security on the Information Highway* (New York: John Wiley and Sons, 1995), 20.
12. Office of Technology Assessment, 1-2.
13. Wired press release, *Wired* 1.3, 1993.
14. "First Computer Wiretap Locates Hacker," *New York Times*, 31 March 1996, 4.
15. Robert L. Ayers, "Information Warfare and the DII," *InfoWar Con Report* (1995):25.
16. Timothy L. Thomas, "Russian Views of Information-Based Warfare" (Ft. Leavenworth, KS, U.S. Army Foreign Military Studies Office, 20 September 1995): 1.
17. 2 and 9 June 1996.
18. Martin Van Creveld, *Command in War* (Cambridge, Massachusetts: Harvard University Press, 1985), 154.
19. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder Mouth Press, 1994), 171-189.
20. Martin C. Libicki, *What is Information Warfare?* (Washington D.C.: Institute for National Strategic Studies, 1995), 49-50.
21. RAND Report.
22. Albert J. Edmonds, presentation to Intelligence and Command and Control Seminar, Kennedy School of Government, Harvard University, Cambridge, MA, 4 April 1996.
23. Goodman, ibid., 20.
24. Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post* 16 July 1995, C3.
25. Defense Authorization Bill of 1996, 104th Cong., 2nd Sess., H.B. 1053.
26. Ashton B. Carter, "Telecommunications Policy and U.S. National Security," in *Changing the Rules: Technological Change, International Competition, and Regulation in Communications* (Washington, DC: Brookings Institution, 1989).
27. Paul Strassman and William Marlow, "Risk-free Access Into the Global Information Infrastructure Via Anonymous Re-Mailers," Harvard Information Infrastructure Project (February 1996), available at http://ksgwww.harvard.edu/~itbspp/anon-remail.html.
28. See David Kay, "Denial and Deception Practices of WMD Proliferators: Iraq and Beyond," *The Washington Quarterly* (Winter 1995).
29. John H. Gibbons, "National Security and the Role of Science and Technology," *SAIS Review*, Vol. XVI, no. 1 (Winter-Spring 1996): 6.
30. Seymour Goodman, Peter Wolcott and Grey Burkhart, "Building on the Basics: An Examination of High-Performance Computing Export Control in the 1990s," Report of the Center for International Security and Arms Control, Stanford University (November 1992): 29.
31. Stewart A. Baker, "The International Market for Encryption - Government Controls on Encryption," Harvard Information Infrastructure Project (February 1996), http://ksgwww.harvard.edu/~itbspp/baker.html.
32. Stuart J.D. Schwartzstein, "Export Controls on Encryption Technologies," SAIS Review, Vol. XVI, no. 1 (Winter-Spring 1996): 29.
33. Richard C. Barth, "The International Market For Encryption - Technology Will Drive Policy," Harvard Information Infrastructure Project (February 1996), http://ksgwww.harvard.edu/~itbspp/baker.html.
34. Baker, 4-5.
35. Jeffrey Larsen and Gregory J. Rattray, *Arms Control Towards the 21st Century* (Boulder, CO: Lynne Rienner Press, 1996), 8.
36. Principal negotiating efforts included the SALT/START treaties including the 1972 ABM Treaty, the 1987 INF, and the 1990 CFE Treaty.

37. Kerry Kartchner, "The Objectives of Arms Control," in *Arms Control Towards the 21st Century* (Boulder, CO: Lynne Rienner Press, 1996), 20.
38. Congressional Budget Office, *U.S. Costs of Verification and Compliance Under Pending Arms Treaties* (Washington, DC: Congressional Budget Office, 1990), xi.
39. Trevor Taylor, "The Arms Control Process: The International Context," in *Arms Control Towards the 21st Century* (Boulder, CO: Lynne Rienner Press, 1996), 43.
40. Stephen Rose, "Hard Choices About Chemical Weapons," in *Essays on Strategy VII* (Washington, DC: NDU Press, 1990): 3-5.
41. Marie Chevrier and Amy Smithson, "Preventing the Spread of Arms: Chemical and Biological Weapons," in *Arms Control Towards the 21st Century* (Boulder, CO: Lynne Reinner Press, 1996), 207.
42. Johnathan B. Tucker, "Strengthening the Biological Weapons Convention," *Arms Control Today* (April 1995): 12.
43. Chevrier and Smithson, 202.
44. Guy B. Roberts, "Five Minutes Past Midnight: The Clear and Present Danger of Nuclear Weapons Grade Fissile Materials," Report for the USAF Institute of National Security Studies (February 1996): 51.
45. Michael Modie, "Ratifying the Chemical Weapons Convention: Past Time for Action," *Arms Control Today* (February 1996): 4.
46. William E. Berry, "North Korea's Nuclear Program: The Clinton Administration's Response," USAF Institute for National Security Studies Occasional Paper #3, USAF Academy, Colorado (March 1995): 3.
47. Jennifer Sims, "The Arms Control Process: The U.S. Domestic Process," Arms Control Towards the 21st Century (Boulder, CO: Lynne Rienner Press, 1996), 69.
48. Taylor, 10.
49. "Convention on the Prohibition of Development, Production Stockpiling, and Use of Chemical Weapons and Their Destruction," *Arms Control Today* (October 1992): 9.
50. Roberts, 18.
51. See Modie, 9, and Rose, 22-23.
52. Mitchel B. Wallerstein, "Concepts to Capabilities: The First Year of Counterproliferation," in Weapons of Mass Destruction: New Perspectives on Counterproliferation (Washington, DC: NDUPress, 1995), 17-26.
53. Thomas, 24-25.
54. Roy Godson and William Olson, *International Organized Crime: Emerging Threat to National Security* (Washington, DC: National Strategy Information Center, 1993), 19.
55. *The U.N. Disarmament Yearbook 1994*, Vol. 19 (New York: UN Press, 1995), 183-184.