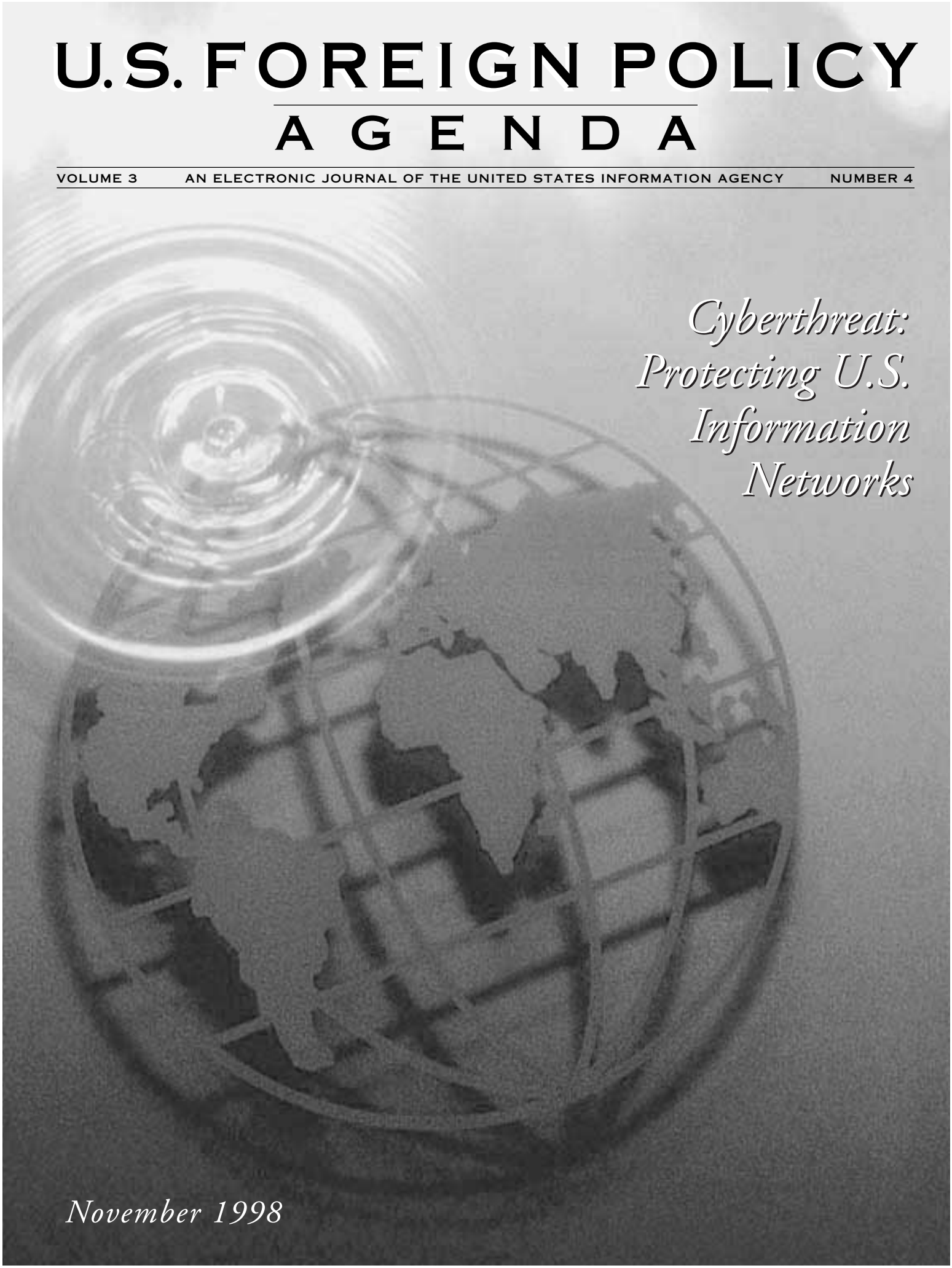
U.S. FOREIGN POLICY AGENDA

VOLUME 3 AN ELECTRONIC JOURNAL OF THE UNITED STATES INFORMATION AGENCY NUMBER 4



Cyberthreat: Protecting U.S. Information Networks

November 1998

U.S. FOREIGN POLICY
AGENDA

Cyberthreat: Protecting U.S. Information Networks

"As we approach the 21st century, our foes have extended the fields of battle — from physical space to cyberspace....Rather than invading our beaches or launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base.... If our children are to grow up safe and free, we must approach these new 21st century threats with the same rigor and determination we applied to the toughest security challenges of this century."

— President Clinton
Commencement Address at the U.S. Naval Academy
May 22, 1998

This issue of *U.S. Foreign Policy Agenda* examines the U.S. response to challenges never before encountered — challenges unique to the Information Age. Key U.S. officials explain initiatives to protect U.S. information networks from cyber attack and to foster government-private sector cooperation in developing security measures. A U.S. senator gives congressional reaction to the debate on information warfare, an academician outlines how universities are responding to emerging national priorities, a private sector expert offers a broad overview of the meaning and evolution of information warfare, and security specialists in the private sector offer insights into how U.S. companies are working with each other and government to meet the security requirements of the cyber era.

U.S. FOREIGN POLICY AGENDA

An Electronic Journal of the U. S. Information Agency

CYBERTHREAT: PROTECTING U.S. INFORMATION NETWORKS

CONTENTS

FOCUS

DEFENDING THE NATION AGAINST CYBER ATTACK: INFORMATION ASSURANCE IN THE GLOBAL ENVIRONMENT 5

By Lieutenant General Kenneth A. Minihan
Director, National Security Agency

INFORMATION ASSURANCE AND THE NEW SECURITY EPOCH 8

By Dr. John Hamre
Deputy Secretary of Defense

CIAO: AN INTEGRATED APPROACH TO COUNTER THREATS OF A "NEW ERA" 11

An interview with Dr. Jeffrey A. Hunker
Director of the Critical Infrastructure Assurance Office

THE YEAR 2000 PROBLEM 16

By John Koskinen
Chairman of the President's Council on Year 2000 Conversion

INFORMATION WARFARE THREAT DEMANDS MORE ATTENTION ON ALL SIDES 18

An interview with Senator Jon Kyl

COMMENTARY

GHOSTS IN THE MACHINES? 21

By Dr. Martin Libicki
Senior Policy Analyst, RAND

THE RESPONSE OF HIGHER EDUCATION TO INFORMATION WARFARE 25

By Dr. Charles W. Reynolds
Director, Department of Computer Science, and Interim Dean, College of Integrated Science and Technology
James Madison University

VIEWS FROM THE PRIVATE SECTOR

PRIVATE, PUBLIC SECTORS BENEFIT BY SHARING EXPERTISE ON SECURITY 29

An interview with Howard Schmidt
Director, Information Security, Microsoft Corporation

STRATEGIES FOR COUNTERING THREATS TO INFORMATION TECHNOLOGY ASSETS 32

By James A. Lingerfelt
Senior Consultant, IBM, Public Safety and Justice

INFORMATION WARFARE: CHALLENGE AND OPPORTUNITY 37
By James Adams
Chief Executive Officer, Infrastructure Defense, Inc.

BACKGROUNDING THE ISSUE

FACT SHEET: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES 40
Presidential Decision Directive 63

A GUIDE TO ADDITIONAL READING

CYBERTHREAT: PROTECTING U.S. INFORMATION NETWORKS, ARTICLE ALERT 42
Abstracts of recent articles

CYBERTHREAT: PROTECTING U.S. INFORMATION NETWORKS, BIBLIOGRAPHY 43
Spotlighting other views

CYBERTHREAT: PROTECTING U.S. INFORMATION NETWORKS, KEY INTERNET SITES 44
Internet links to resources on related issues

U.S. FOREIGN POLICY
AGENDA

AN ELECTRONIC JOURNAL OF THE U.S. INFORMATION AGENCY VOLUME 3 • NUMBER 4 • NOVEMBER 1998

Editor, U.S. Foreign Policy Agenda
Political Security - I/TPS
U.S. Information Agency
301 4th Street, S.W.
Washington, D.C. 20547

E-mail: ejforpol@usia.gov

Please note that this issue of U.S. Foreign Policy Agenda
can be located on the USIS Home Page on the World Wide Web at "http://www.usia.gov/journals/itps/1198/ijpe/ijpe1198.htm".

DEFENDING THE NATION AGAINST CYBER ATTACK: INFORMATION ASSURANCE IN THE GLOBAL ENVIRONMENT

By Lieutenant General Kenneth A. Minihan
Director, National Security Agency

The National Security Agency "is applying its unique expertise to develop the fundamental technology to create a national cyber-attack detection and response capability," says Air Force Lieutenant General Kenneth A. Minihan. He emphasizes that "information superiority in the Information Age is a clear national imperative."

"We are at risk. America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans, to criminal records. Although we trust them, they are vulnerable — to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

— "Computers at Risk," National Research Council, 1991

INTRODUCTION

Perhaps the most remarkable thing about the words quoted above is that they were written almost at the dawn of the Information Age. Until recently, we as a nation have paid them little heed. The United States, and the rest of the world, continue to charge headlong into the information revolution — information technology is making profound inroads into the very fabric of our society and our economy as a nation in the global community. In a very real sense, the "Information Superhighway" has become the economic lifeblood of our nation.

While leading the world into the Information Age, at the same time the United States has become uniquely dependent on information technology — computers and the global network that connect them together. This dependency has become a clear and compelling threat to our economic well-being, our public safety, and our national security.

The world's networks, referred to by many as "cyberspace," know no physical boundaries. Our increasing connectivity to and through cyberspace increases our exposure to traditional adversaries and a growing body of new ones. Terrorists, radical groups, narcotics traffickers, and organized crime will join adversarial nation-states in making use of a burgeoning array of sophisticated information attack tools. Information attacks can supplement or replace traditional military attacks, greatly complicating and expanding the vulnerabilities we must anticipate and counter. The resources at risk include not only information stored on or traversing cyberspace, but all of the components of our national infrastructure that depend upon information technology and the timely availability of accurate data. These include the telecommunications infrastructure itself; our banking and financial systems; the electrical power system; other energy systems, such as oil and gas pipelines; our transportation networks; water distribution systems; medical and health care systems; emergency services, such as police, fire, and rescue; and government operations at all levels. All are necessary for economic success and national security.

INFORMATION ASSURANCE — THE NATIONAL GOAL

On May 22, 1998, the president signed Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection. In it he states: "I intend that the United States will take all necessary measures to

swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

The national goal is that by no later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

— The federal government to perform essential national security missions and to ensure the general public health and safety;
— State and local governments to maintain order and to deliver minimum essential public services;
— The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services."

Achieving this sweeping goal will be a considerable undertaking, requiring a cooperative effort between the government and the private sector elements that operate the critical infrastructures. The PDD directs the federal government to lead by example in assuring the robustness of federal systems, but also makes it clear that the public sector cannot solve the problem unilaterally. Every federal department and agency is highly dependent on the services provided by the private sector — power, telecommunications, transportation, etc. Thus, the PDD envisions a Public-Private Partnership to develop and implement a comprehensive National Infrastructure Assurance Plan, to deal with the threat of electronic terrorism. The significant challenge is how to get the private sector to engage infrastructure assurance from a national perspective. In today's highly competitive environment, the private sector is typically driven to achieve market advantage — including driving down operating costs — to increase profits. Enhanced cyber-protection measures will require both expanded investment and collaboration with competitors.

ESSENTIAL ELEMENTS

Any strategy for enhancing the robustness of our critical infrastructures must contain three basic elements: increased protection against cyber attack, the ability to detect when an attack is occurring, and the capability to respond and/or recover when an attack is detected.

Increased protection against cyber attack is founded upon encryption technology — including digital signatures — to provide the authentication, integrity, non-repudiation, and privacy/confidentiality services necessary for information assurance. Strong digital-signature-based authentication used to provide positive access control is perhaps the most powerful tool in protecting against cyber attack. Digital signature also provides for integrity of electronic information and non-repudiation of cyber-transactions. Encryption is applied to desktops, file servers, and across networks to assure the privacy of sensitive government, business, and personal information. Once the almost exclusive province of governments, encryption technology is now widely available in the commercial marketplace, and is a fundamental enabler for information assurance. In fact, on September 16, 1998, the vice president announced a major updating of U.S. Export Control Policy on Encryption Technology, a clear indication of its importance to critical infrastructure protection, as well as global electronic commerce and economic prosperity.

Given the coming of age of encryption technology, the remaining challenge is to apply the technology in a coherent and effective way to all of our critical infrastructures. To do this requires both a framework for application of the encryption services in a scalable, interoperable way, along with the establishment of a supporting public key infrastructure (PKI) to provide robust and globally recognizable digital signature and encryption key certificates, the individually unique "electronic ID" of the Information Age. PKI services are now emerging in the private sector to meet the demands of global electronic commerce and can be leveraged to support critical infrastructure protection.

In the areas of diagnosing, detecting, and responding to cyber attack, the technologies are not so mature or effective. Today, the United States has little ability to detect or recognize a cyber attack against either government or private sector infrastructures, and even less capability to react. The ability to identify a strategic cyber attack against one or several critical infrastructure components, and respond in appropriate fashion, is clearly a significant national security issue.

One complicating factor is that computer intrusions have been traditionally regarded as a criminal event and within the purview of law enforcement. When an intrusion occurred, the intruder was (hopefully) tracked down, arrested, and prosecuted. Further, many private sector entities were reluctant to share information about computer intrusions, fearing adverse press coverage (e.g., newspaper headlines such as "Bank Losses Put at Millions in Computer Break-in" or "Hackers Disrupt Telephone Service") and public reaction. To build an effective national cyber-defense capability, new rules of engagement must be developed to allow open and dynamic collaboration among the private sector, the law enforcement community, and the national security community.

EMERGING INFORMATION ASSURANCE ROLE OF THE NATIONAL SECURITY AGENCY

In the Information Age, the National Security Agency's traditional missions of Signals Intelligence and Information Systems Security are evolving into one of providing information superiority for the United States and its allies. Central to this construct is an in-depth understanding of the Global Information Infrastructure and the vulnerabilities of networked information systems to cyber attack. On the defensive side of this mission, the NSA has undertaken a series of initiatives to provide the technical foundation to protect our critical infrastructures.

As mentioned earlier, encryption technology has become widely available in the commercial marketplace and is the basic foundation for protecting information systems from cyber attack. The bad news is that the many products available do not securely interoperate with each other and are of varying robustness, and that there are many, often confusing, ways to apply encryption. As an example, there is e-mail encryption, file encryption, web encryption, link encryption, and virtual private network encryption, just to name a few of the variations. To remedy this situation, the NSA has formed a partnership with the leading suppliers of security-enabled information technology to develop a common framework for encryption services to provide enterprise-wide information assurance solutions. This framework defines a coherent way to apply encryption technology to the enterprise, along with how encryption interacts with and supports other security-related technologies and products, e.g., firewalls, servers, routers, operating systems, intrusion detection, malicious code detection, audit tools, and public key infrastructure services.

Another dimension of the problem is the varying degrees of robustness in the many security relevant products in the marketplace. To address this issue, the NSA has formed a partnership with the National Institute for Standards and Technology (NIST). Under this arrangement, the NSA and the NIST will certify commercial laboratories to evaluate commercial security relevant products, either to validate the vendor's security claims, or to validate compliance with the requirements of the network security framework. Testing of the products will be done by the certified laboratories on a fee-for-service basis, with cost and schedule negotiated between the lab and the product vendor.

Lastly, the National Security Agency believes the nation needs a shared array of national security information assurance elements and is applying its unique expertise to develop the fundamental technology to create a national cyber-attack detection and response capability. The approach integrates a variety of sensors that can be applied at critical infrastructure locations and in the underlying telecommunications infrastructure itself, with sophisticated, broad-scale analytic techniques to provide a dynamic view of the threats to critical infrastructures from global cyberspace. These techniques should be shared by an array of national security, federal, industry, and regional components to allow concurrent detection, defense, reconstitution, and recovery of vital services.

IN CONCLUSION

The economic prosperity that our nation enjoys today is largely founded in the Information Age and in our global leadership in information technology. Our continued leadership and prosperity in the global economy may well hinge on our national commitment to act as leaders in bringing integrity and responsibility — information assurance — to the global information environment we have helped to create. The administration has sent a clear message via PDD-63 that the time to act is now, and the NSA is well-positioned and ready to support the charge with our technical know-how. Information superiority in the Information Age is a clear national imperative. ◉

INFORMATION ASSURANCE AND THE NEW SECURITY EPOCH

By Dr. John Hamre
Deputy Secretary of Defense

Protecting critical information resources will become "one of the defining challenges of national security in the years to come," says Deputy Secretary of Defense John Hamre. Noting that the Pentagon is charged with protecting 28,000 different computer systems, he warns that securing the virtual world from cyberthreats "is as much a process of management approach and attention as it is of technology."

The United States has faced five security epochs, with each change involving transitions from a certain past to an uncertain future. The first epoch was from the Revolutionary War to the mid-1820s, with the United States at the fringe of an international security environment still dominated by Europe.

From the mid-1830s to the end of the 19th century, we enjoyed the insulation of the Atlantic Ocean to tend to our own affairs as the old European political construct disintegrated. This second epoch ended with World War I and the emergence of the Soviet Union. A third epoch took place from 1920 to 1946 and was characterized by global recession and the rise of international communism as Europe collapsed. These events led to a crisis for American democracy and the free enterprise system with the Great Depression, and the tensions in the international security environment led ultimately to World War II.

The most recent epoch — the Cold War — was dominated by a bipolar world. The United States led the international community in creating institutions to rebuild the shattered economies of Europe and to deal with the collapse of the old Europe-dominated empires in the Third World. At the same time, the United States was leading the free world states to contain communism until the Soviet Union collapsed.

Now we are in transition to a new epoch, seemingly characterized by the revival of old dangers — nationalism and ethnicity. Another dimension in this new epoch is the dissolution of control and spread of the technologies that were created in the last epoch and the dramatic ascent of startling new technical capabilities that hold heretofore unheard of potential for both good and evil. We now live with the unsettling fear of "loose nukes" and chemical and biological weapons in the hands of terrorists.

The next security epoch also will present the challenge of cyber security. The explosive growth in the use of information technologies (IT) has had a profound effect on all sectors of the American economy and government. IT has fueled amazing economic growth, dramatically improved communications, and allowed American businesses to compete more effectively than ever. The United States — and the world — truly rely on information technology in ways unimaginable even just a few years ago.

Nowhere is this more true than in the U.S. military. The Department of Defense (DOD) is using IT to bring about what we call a Revolution in Military Affairs — the movement and use of vast amounts of information to provide more reliable intelligence, radically improved command and control, better business practices, and more powerful weapons systems. This revolution is vital if we are to remain ready to defend U.S. interests today and prepare for the evolving threat of the next security epoch.

The IT revolution is infusing every corner of DOD, both in the field and in the headquarters. Soon our soldiers at the squad level will have communications that allow commanders to know precisely the individual soldier's position, situation, and even heart rate — almost complete "battlespace awareness." Our sailors send e-mail home from ships at sea after using very similar technology to target cruise missiles. Pilots now factor in the "task saturation" of the flood of information available to them in flight.

In our logistics processes, technology is being used to connect the front lines to the supply lines. We are committed to a paper-free acquisition process by the turn of the century. We have opened our Joint Electronic Program Office to streamline unit-level purchasing and are now using Internet-based electronic "shopping malls" to buy everything from pens to hydraulic actuators. We are using the Internet for a spectrum ranging from travel payments to satellite communication, and we have made huge strides in electronic publishing.

In short, DOD is harnessing the power of the microchip to build the military of the 21st century. As we do so, however, we also must recognize that with new technologies come new dangers. The same technologies that allow us to seek new efficiencies can also be used by those who cannot attack us on the conventional field of battle to attack us in cyberspace. This is part of a very different and very important dimension in national security thinking; technologies and capabilities once accessible only to large nation-states are now accessible to individuals. The protection of our information resources — information assurance — will thus be one of the defining challenges of national security in the years to come.

There is little argument that information assurance is critical; we in DOD already have seen the first wave of cyberthreats in both exercises and actual attacks. To start to learn the extent of our vulnerabilities, last year we conducted an exercise. Our "enemy" was a group of about 35 people who had the mission to break into DOD computer systems. Their tools were limited to commercially available, off-the-shelf technologies and software that was sold on the open market or downloaded off the Internet. Within three months, the group, operating under those constraints, was able to attack us, penetrate our unclassified networks and, in fact, could have seriously disrupted our communications and power systems.

Last February, we experienced an organized attack against computer systems in the Pentagon at a time of increasing deployments to the Persian Gulf. It turned out to be by two teenagers in California, but coming when it did, the attack could have been much more serious. Both our exercise and small-scale attacks have served as wake-up calls that more serious attacks are not a question of "if," but "when" and "where."

To deal with these threats, we must first consider our mindset. Americans have traditionally thought of security like a fence around a yard, setting borders and protecting the area inside. If there is a break in the fence, it can be fixed and made secure again. This thinking worked well in previous security epochs, but there are no borders in cyberspace. The transition to the epoch to come must be marked not only by advancement of technology, but also by flexibility of thought. We must realize that security in the virtual world is as much a process of management approach and attention as it is of technology.

Changing mindsets can be among the most difficult of tasks. Without realizing it, we are now, for example, providing information to potential foes that they previously spent hundreds of millions of dollars in intelligence operations trying to acquire. We had one military installation with what was thought to be a great homepage on the Web. It showed an aerial view of the facility with buildings labeled "Operations Center" and "Technical Support Center." It was great public relations, but it also provided valuable targeting information for those who might wish us ill.

With an understanding of the broader issues involved with information assurance, we must move to take tangible action to protect our information resources. Within the past year, DOD has pulled together disparate efforts to try to understand the requirements to protect our information infrastructure. The pace of IT advancement makes this a daunting challenge; DOD has 28,000 different computer systems, all of them being upgraded and changed, and we must understand their vulnerabilities. The challenge of information assurance is akin to war, and we are approaching it that way by designating a Joint Task Force Commander for Computer Network Defense to organize our efforts. DOD is also a key contributor to the National Information Protection Center and the President's Critical Information Assurance Office.

Other actions are needed as well. Ninety-five percent of our communications are now over public telephone and fax lines, which makes encryption a core element in information assurance. One of the most dangerous scenarios in the virtual world is that our warfighters will receive deceptive "spoofed" messages that mislead them, so without reliable encryption, the entire

information infrastructure on which we depend is vulnerable. In response to this threat, we are now working to ensure that within DOD, we can guarantee the digital identity of users and develop a reliable public key system. We must strengthen our encryption processes so that the information we transmit and deal with electronically is secure and verifiable.

DOD is also making important strides in broader network security. We are installing network monitoring capabilities and working to ensure configuration control over an inherently changing and dynamic network environment. We are installing firewalls, network monitoring centers, digital signatures, and a security infrastructure.

Information assurance, encryption, and network security pose some of the most daunting challenges the Department of Defense has ever faced. To take advantage of the IT revolution, we must ensure access to and protection of the very assets on which we depend. We are taking giant strides to make this happen, but much more remains to be done. These challenging days require that we turn to the expertise of information professionals both in DOD and in the broader government and private sectors to protect systems vital to all of us. We must ensure that our nation's journey into the new security epoch is as successful as the last.

CIAO: AN INTEGRATED APPROACH TO COUNTER THREATS OF A "NEW ERA"

An interview with Dr. Jeffrey A. Hunker
Director of the Critical Infrastructure Assurance Office

"The full support of the private sector" is vital in protecting U.S. critical infrastructures against cyber attack, says Dr. Jeffrey A. Hunker, Director of the Critical Infrastructure Assurance Office (CIAO). "The threat that we are facing is a threat that's growing over time," he says. "And so we need to respond with a sense of urgency and produce real results very quickly to combat it." Hunker was interviewed by Contributing Editor Susan Ellis.

Question: As director of CIAO you are charged with bringing together an integrated national plan for addressing physical and cyberthreats to the nation's communications, transportation, energy, and other vital infrastructures. What is the key challenge you face as you carry out your new responsibilities under this initiative announced by President Clinton last May?

Hunker: The key challenge that the president has recognized is that we now live in a new era where there are threats that we have not faced before. Specifically, we live in an age now where — because telecommunications and the Internet are so interconnected with the electrical power system, our basic transportation and telecommunications systems — there is a vulnerability to disruption of these systems by what we call cyber attack, using computers, using the Internet to hack into systems and disrupt them, take them down. Such an attack not only could interfere with, for example, military operations, it also could disrupt any vital services that the economy depends on and that Americans depend on — such as electric power, use of telephones, basic transportation services.

It's a completely new challenge that has evolved because of the technology, the interconnectedness of the American economy. The basic challenge that we're facing is one of educating Americans about this new threat and of working with the business sector, key industries, to ensure that we have the protections in place against these types of cyber attacks.

Q: It really is completely new, isn't it?

Hunker: Yes. We have in the past 10 years successfully wired together the economic sectors of the nation, and that has brought great benefits in terms of economic growth and the sort of prosperity that America has enjoyed. But with that new prosperity also has come a new vulnerability and — whether it be nations or terrorist groups or criminal cartels that wish us ill — this new vulnerability that comes from our dependence on electronic systems and information-based systems is a new way in which we can be attacked.

Q: What agencies of the government are involved in the effort to counter this threat, and how does your office work with them to carry out your mission?

Hunker: There are 11 major agencies in the federal government that the president has charged to work together. Key ones include the Defense Department and associated agencies; the intelligence community; and law enforcement — the Federal Bureau of Investigation, the Secret Service, and the Department of Justice. And I think also very important are the Commerce Department, the Treasury Department, and the Transportation Department. They have all been asked to work together in creating a national plan.

But even more important, they have been asked to work together with the private sector. Because almost all of the so-called critical infrastructures that are vulnerable to attack, in fact, are owned by the private sector. And if we don't have the cooperation and the full support of the private sector in developing this capability to protect ourselves, we're not going to get very far.

Q: How will you measure the success of your mission?

Hunker: That's difficult, because it's a new challenge, and because, in many ways, the types of attacks and

threats the president has asked us to protect the nation against are evolving, are really new. In some cases they haven't happened yet, and measuring success here is going to be difficult. I think that one major measure of success is going to be the extent to which the private sector — the owners and operators of the electric power grid, and our transportation and our banking and finance sectors — comes together and, with the government, develops an action plan. We'll be able to measure how that partnership has been formed within the next six months to a year. That's really the first major measure of success.

Q: What time frame are you trying to meet?

Hunker: It's a tight time frame because the threat that the president is concerned about — coordinated, sophisticated electronic attacks against the nation's critical infrastructures — is one that is out there right now. The president has called for a national plan with an initial capability to protect against the new types of cyber attacks by the year 2000. And he has called for, by the year 2003, a full operating capability to protect the nation. The threat that we are facing is a threat that's growing over time. And so we need to respond with a sense of urgency and produce real results very quickly to combat it.

Q: I understand that you plan to have something ready in November.

Hunker: That's right. Actually one of the very first steps that the president called for in his announcement in May was that within six months, which is the middle of November, agencies of the federal government will have made important progress toward developing their own plans to protect their own critical infrastructures. This means that, among others, the Treasury Department and the Department of Defense will have a process for establishing defenses to protect themselves against electronic attack. Secondly, the president called for us to have laid out the milestones for a larger national plan that will involve working very closely with the private sector, integrating the work of a number of different agencies, and bringing in the university and research communities and the like; so there are many different elements. We won't have the national plan in place in November, but we will have established important milestones in terms of building that national plan.

Q: How would you assess the nature and gravity of threats to U.S. critical infrastructures, and what sectors are most vulnerable?

Hunker: To understand the threat to, and the vulnerability of, U.S. critical infrastructures, we really have to start with an understanding of how the economy has developed. Over the past couple of years, with the growth of the Internet, which is doubling in its usage and size every 10 months, vital basic services that Americans depend on — things like electric power, our banking system, our telecommunications system — are all interconnected. Those systems are the basis for economic growth and for supporting vital national security missions, and they are all very vulnerable right now.

We had an instance early this year where, during the buildup in response to Iraqi actions, there were indications that hackers were breaking into sensitive Department of Defense computers. That concern occupied the highest levels of government for several weeks while people were examining the sources of this attack. Was it coming from Iraq or its allies? It turned out that it was two teenage hackers in the United States, supported by somebody in another country who was giving them advice. But that gives you an indication in terms of the sorts of vulnerabilities that we have.

A teenage hacker, again, in Massachusetts, took down a large portion of the Massachusetts telephone network and in so doing actually made a major airport electronically blind for a period of time, causing real threats to the safety of air travel. If single hackers can do that sort of damage, imagine what a sophisticated, organized attack that's designed to take down major portions of our electric system or our telecommunications system or break into sensitive computers could do. That's the nature of the threat that we're dealing with. And there are a lot of indications that suggest that people in other countries are aware of, and are developing, this sort of offensive capability to attack America electronically.

Q: As CIAO director, you are coordinating a national education and awareness program. What is your message and how are you relaying it to the citizens of the United States?

Hunker: It's very important that, as we talk about education and awareness, we consider two different

messages. One is awareness. We are dealing with a new age, and this is a new type of threat that has only recently become the subject of a lot of concern. Therefore awareness is clearly part of the message. I have been very pleased, though, because — in talking across the government at the Cabinet level and very senior level — people understand the nature of the threat. And senior business leaders and senior university leaders already understand this.

Our second message is: What can we do about this? And that's why we are building the partnership between private industry and the different parts of the government to take real action in the coming months, and then obviously in the coming years, to respond to this.

Q: How would you describe the extent to which we have become dependent on computers, not only in our personal lives but for the basic functioning of our society?

Hunker: Look in your house, look in any office that you use. What you see is our dependence on electronic systems. We go to the bank and we use the automatic teller machine; that's an electronic system that's wired together nationally and internationally. Our electric power grid is all being managed increasingly, in fact, using the Internet. Air transport and railroads are all dependent on electronic systems. Even companies that you don't think of as being computer or software companies — their operations and productivity depend on information systems that are wired together.

It's estimated that between one third and one half of the economic growth that this country has seen for the last couple of years, with hundreds of thousands of jobs being created, is coming from electronic commerce. This is the basis for our economic growth in the future; it's also the basis for supporting our national security mission, whether it be moving material and personnel around the world, or whether it be in terms of collecting vital information and intelligence on threats. This is all based at its core on these new electronic systems.

Q. How are you working with the private commercial and industrial sectors to enhance the protection of U.S. information and communications networks?

Hunker: Working very closely with the private sector is really core to the goal and the mission that the president has set out. It may be apocryphal, but it's pretty accurate that 90 to 95 percent of Defense Department communications systems are in fact privately owned and operated. It's vital. Unless we engage the private sector, we're not going to get very far.

I am now involved in a series of meetings with other senior government officials from different departments — including the Treasury Department and the Transportation Department — and with private sector leaders in the critical infrastructure industries of banking and transportation, for example, as part of the collaborative effort to build the partnership between government and the private sector.

In September I was in Charlotte, North Carolina, meeting with the mayor and other city and county officials, as well as with the senior executives from some of the major banks. Charlotte is the number two banking center in the nation. And the purpose of my visit was to make certain that the major banks in Charlotte are part of the partnership.

We have plans under way for a series of meetings later this fall that will involve the president, the vice president, and the national security adviser, together with the leaders of the electric power sector, banking and finance sector, transportation and other critical infrastructures to really further build this partnership.

It's a long process. Building partnerships, particularly in an area where we haven't been working together before, doesn't happen overnight. I have been very pleased, though, with the sort of response and awareness and real cooperation that I have seen from CEOs (chief executive officers), from chairmen, and from senior executives in all of the industries that I have been working with.

Q: Is CIAO involved with university communities and programs to help find improved ways to secure U.S. information and other critical infrastructures?

Hunker: The university community is going to be another important part of the sort of partnership that we're dealing with. In fact, in September, I personally met with the chancellors and deans of several major universities — the University of North Carolina, Purdue University, the Massachusetts Institute of

Technology, the University of Virginia, just to name a few. And the reason is really twofold. Right now in this country we have a vital shortage of computer specialists and information technology specialists. And the threat of cyber attack is simply going to increase the shortage that we're facing. It's going to increase the demand for people who have training. And it's going to be the universities that are at the front line of training the sorts of people that we're going to need.

We're also going to need the sort of research and development that will develop new solutions, develop new technologies for protecting our information systems. And universities are going to be a key part of that.

Q: As CIAO director, you have the responsibility to develop legislative initiatives. How are you interacting with the U.S. Congress and how do you assess the congressional impact on policies and strategies related to CIAO objectives?

Hunker: Working with Congress is a very important part of this agenda. And I would say that congressional interest has been extremely high, and Congress has been extremely supportive of addressing this new form of terrorist or national security threat. I would anticipate that there are going to be several major issues on which we're going to continue to work with Congress, clearly in terms of resources.

As part of the work that we're doing, we're anticipating the president will include in his fiscal year 2000 budget a major initiative for protecting critical infrastructures. That will include resources for research and development; it will include resources for new initiatives to train information technology specialists, both for the federal government and for the private sector, and perhaps other initiatives. So support on the resources side is going to be very important.

Congress also will be looking at the existing set of laws that deal with computer security. A hacker often will go through a number of different computers before he ends up finally at the computer that he actually wants to break into. The way the law works right now, if you want to track where that hacker has been — and he has been in different states — you have to get different search orders from judges all across the country to be able to do that work. We're going to be working closely with the Congress to look at the sorts of legal procedures and protections that now exist.

Q: Do you see the need for greater international collaboration and cooperation in protecting key infrastructures, and if so, how can this be achieved?

Hunker: The international aspect is one that cuts through everything associated with the cyber world. We're talking about a threat that can come from overseas; it also can come domestically. But this sort of threat doesn't necessarily require people to be close to the institution or the infrastructure that they are attacking.

We had a situation in the past year where there was a hacker in Germany who was in fact an Indian citizen, hacking into a financial system in Miami in an attempt at extortion. So here we have two countries and the citizens of three countries essentially involved in an incident that was directly attacking a U.S. institution. It just gives you a small example in terms of the international aspect of all of this.

The President's Commission on Critical Infrastructure Protection issued its report last year after looking for two years at this issue. Its recommendations were key to the framework that the president announced in May. It recognized the international dimension as being a very important one.

The president has tasked the State Department to take the lead in our discussions with other countries in terms of information-sharing and in terms of the potential for new treaties or protocols for responding to the sorts of terrorist or other attacks that might happen. We've already had expressions of interest about this from a number of countries. I've met personally with representatives of the Canadian government and the Mexican government, and I know that discussions have taken place in the context of NATO and other international organizations about this issue.

So, there is a lot of interest, but we're at a very early stage in terms of how the international agenda is going to be developing.

Another important issue is the overlap between the work to protect against cyber attack — whether it

comes from organized crime or from terrorist groups or from other nations — and what's called the year 2000 (Y2K) computer problem. Y2K is different because we know exactly when the problem is going to happen. And this is something that we did to ourselves, because, years ago, computer programmers didn't factor in that the year 2000 would have a different set of dates than the year 1900. (Many older computer systems use only the last two digits of a year to keep track of the date.)

But in many ways addressing the Y2K threat requires exactly the same set of actions as protecting against cyber attack. Institutions, companies, the federal government have to start by identifying what systems they have and how are they interconnected, and then decide which systems are the most important to protect and how to protect them.

Another aspect of the year 2000 problem that overlaps with the threat of cyber attack is the creation of a nationwide capability to respond and rebuild systems if something goes wrong in the year 2000. That's going to be the model for a nationwide capability to respond against cyber attack as well. It will involve key industries, state and local emergency responders, and the key parts of the federal government. And, in fact, my office works very closely with John Koskinen, the special adviser to the president for year 2000 issues, on various aspects of this overlapping agenda for Y2K and cyber issues.

THE YEAR 2000 PROBLEM

By John Koskinen
Chairman of the President's Council on Year 2000 Conversion

The head of the U.S. government's effort to deal with the year 2000 computer problem says the major obstacle to overcome is "insufficient awareness" about the problem "among government leaders, journalists, business executives, and the general public" around the world. He fears that "inactivity and lack of awareness could lead to fulfillment of some worst-case scenarios." But he stresses that "by taking action now we can minimize the disruptions and, hopefully, effect a seamless transition to the year 2000."

The world currently faces one of the great challenges of the Information Age. As we head toward a new millennium, many computer systems, as well as the computer chips embedded in everything from personal computers to household appliances and sophisticated manufacturing equipment, are set to shift backwards in time.

The problem is that many older computer systems and microprocessors, as computer chips are known, use only the last two digits of a year to keep track of the date. So, when the year 2000 arrives, those chips may recognize 00 as the year 1900, not 2000. The resulting malfunctions could cause serious disruptions of power grids, water treatment plants, financial networks, telecommunications systems, and air traffic control systems worldwide. In an increasingly wired world with a global economy, computer networks are only as strong as their weakest link. While each nation is likely to experience its own particular system problems, in a very real sense we are all in this together.

Why did software designers make such an obvious mistake? Thirty years ago computer memory was in much shorter supply than at present, so computer programmers relied on shortcuts like the two-digit year to save memory. Their assumption was that the programs they designed would be outmoded and replaced by new software long before the year 2000. In practice, however, many large, complicated computer systems such as those used by banks, insurance companies, or stock brokerage firms have evolved over time, with the latest software added onto existing systems. Consequently, any organization that operates large-scale, interconnected computer systems will have to check millions of lines of computer code to determine how dates are handled, then rewrite software to correct the problem, then run these applications to see how they work, and then check each program's interface with the internal and external applications it uses.

The technological fix is not difficult, but because of the sheer scale of the year 2000 problems, we face an enormous organizational and management challenge. Just to cite one example — there is a limited labor pool of those qualified to fix the problem, programmers skilled in computer languages that may have become obsolete years ago.

To coordinate work on this problem within the U.S. government's many systems, President Clinton has formed a council of more than 30 agencies. Our first goal is to maintain basic government services — to ensure that health-care and unemployment benefits continue to be paid, that tax collections are not disrupted. The president's ambitious target is to have 100 percent of U.S. government systems "year 2000 compliant" — that is, fixed — by March 1999. The council also has working groups devoted to interacting with state and local governments on this problem and assessing private companies' efforts in 35 industrial sectors, such as transportation, telecommunications, and finances.

In addition, we are concerned about the state of year 2000 efforts in other countries since many computer systems cross national borders and, in a global economy, no nation is a digital island unto itself. We are working through international agencies to address the problem. The United Nations passed a resolution

that called on all member states to take action and report back to the General Assembly by October 1. The World Bank has held 20 regional conferences to raise awareness of this issue. The International Monetary Fund has agreed to use all its influence to encourage countries to devote resources to the problem. Secretary of State Madeleine Albright has sent a cable to U.S. embassies around the world, instructing the ambassador to make inquiries of each host country about the level of its preparedness for the year 2000. The U.S. Information Agency heads up a working group of the President's Council whose mission is to raise awareness, act as an information gateway, and focus on contingency planning with other countries.

Unfortunately, at this point fewer than 500 days until January 1, 2000, I find that the biggest problem is still one of insufficient awareness among government leaders, journalists, business executives, and the general public in many countries. The first step is for nations and private companies to inventory all their operations involving computers and develop a plan for fixing them. A second vital step is contingency planning. The President's Year 2000 Council has asked each U.S. government agency to develop two kinds of plans: one, what will we do if some of our computer systems don't work? The second level is outside contingency planning: what will we do if systems interconnected with our systems fail?

Year 2000-related disruptions are likely to begin before the new millennium as outmoded systems attempt to calculate or schedule future events. Precisely what will happen is difficult to predict at this point. There are a number of Internet Web sites in the United States where some experts that one would not normally think of as alarmists have predicted widespread system failures that will result in power outages, traffic problems, economic recession, and possibly, in some regions, food shortages. While I tend to be more optimistic than these doomsayers, I am concerned particularly about countries where inactivity and lack of awareness could lead to fulfillment of some worst-case scenarios. The point is that by taking action now we can minimize the disruptions and, hopefully, effect a seamless transition to the year 2000.

INFORMATION WARFARE THREAT DEMANDS MORE ATTENTION ON ALL SIDES

An interview with Senator Jon Kyl

Neither the administration, nor the Congress, nor the public at large is devoting enough serious attention to the growing threat of information warfare, says Senator Jon Kyl. Potential adversaries are honing their ability to attack the critical infrastructure that increasingly runs the nation's communications, transportation, and financial systems — and its vital defense establishment as well, he warns. Kyl, an Arizona Republican, serves as chairman of the Subcommittee on Technology, Terrorism, and Government Information of the Senate Judiciary Committee. He also is a member of the Senate Select Committee on Intelligence. Kyl was interviewed by Contributing Editor Ralph Dannheisser.

Question: At a committee hearing in June, you said that the United States' "soft, digital underbelly" is more readily vulnerable to attack than the nation's military. Could you elaborate on that a bit?

Kyl: I think that's generally recognized as true. We've got the strongest military in the world, and there's nobody that's really capable of taking us on. So the question is: Would a potential adversary seek the more vulnerable spots to attack the United States if they wanted to do so? The same thing for terrorists. And the answer is that among the vulnerabilities that we have is our information infrastructure, because we are reliant more than any other nation on high technology for our communications, our transportation, our financial dealings — including, of course, our defense establishment. And as a result, the vulnerability that our information infrastructure has is probably one of those key target points for either an aggressor state or a terrorist organization.

Q: Along the same lines, you have said that this is the most difficult and important national security and public safety concern that our country's leadership will face in the years ahead. What are some of your worst-case fears if the issue is not properly addressed?

Kyl: Let's start with the transition to the new millennium. The Y2K (year 2000 computer) problem, which has been rightly identified as a serious potential problem for the country, is exacerbated by the fact that it will present terrorists or other groups of people or individuals who mean us harm a golden opportunity to attack at the time of maximum confusion. We will not know why the many things that are going wrong at midnight, December 31, 1999, are going wrong. We will presumably attribute most of the problems to Y2K computer glitches, but obviously it represents a great opportunity for sabotage or other attack on our infrastructure by those who mean us harm — both because their activities are covered by the event and also because of the vulnerability that the event itself presents.

So there's the first great opportunity. But apart from just that moment in time — because, as I said, of the vulnerability of the different aspects of our civil society as well as certain defense components — attacking our infrastructure represents one of the best ways of doing us harm in the abstract and, in a situation where there is an ongoing conflict, represents a great opportunity to disrupt our ability to meet the threats involved in that contingency.

Q: Overall, how easy is it to break into the information grid at some point, and what sort of damage could someone who succeeds in that effort do?

Kyl: Well, it's surprisingly easy. It's hard to quantify that in words, but there have been some exercises run recently. One that's been in the media, called "Eligible Receiver," demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers — people using conventional equipment, no "spook" stuff in other words. Just that which is available can disrupt key aspects of

our information infrastructure. Now, in this case, they disrupted parts of the electric grid, the transportation system, the financial system. Others that are vulnerable include things like water systems, all forms of telecommunications, of course, and the emergency response people, but perhaps from the defense point of view nothing is more serious than the labs of the defense establishment itself as well as weapons systems.

So, there is a high degree of vulnerability, and each time some youthful hacker from another country breaks into the Pentagon computer system, people scratch their heads and wonder how it can happen and they learn from the exercise. But it seems that it's a constant learning process. Another illustration: just before the dust-up last February in Iraq, where we were about to go in and do something to Saddam Hussein, the hacking into the Pentagon computers was so significant that the president was actually advised that the activity could be the result of an intentional action by the Iraqi government. For a while we did not know whether that was the cause of this or not. It turned out to be three young men in three different countries. So to respond to the question — "How vulnerable are we?" — I think that helps to illustrate the point.

Q: Certainly the fact that these young guys with no sinister motives can get in that easily would suggest that our adversaries could do it as easily with significantly more prospect of damage.

Kyl: That's exactly the concern.

Q: From your own perspective with the committee and having a keen interest in the topic, how do you see the Congress' role in protecting against this sort of information warfare or cyberterrorism?

Kyl: Well, the obvious — we have to give the national security agencies, the defense establishment, enough money to deal with the problem and the authority to deal with it.

There are some real issues involved, but I think that from a public policy standpoint, it's primarily to establish the policy for the government, to take it seriously, and to provide the means of doing so.

Now, we have been prodding the (Clinton) administration for four years, and it's still behind the curve. It was supposed to present a plan, and that hasn't been accomplished yet. What the president did, in an executive order, was to order in 180 days a plan to be prepared. So we're awaiting that. November 22 would be the due date. So presumably that's the agencies' plan for dealing with this among themselves.

Q: That was at the instigation of the Congress?

Kyl: The Congress got the ball rolling, by twice requesting, or requiring, the president to submit a plan or a report. He didn't do that. Instead he appointed a commission, first of all, and as part of that he also appointed a task force within the government. Among the recommendations that they made was to prepare this plan. And so they've been planning to begin to commence to start to report here for a long time, and we're about to the end of that 180-day process now. I'm hopeful that that plan will at least provide the direction for each key government agency, in dealing with the private sector that it has relationships with, to provide the guidance for at least the first phase of activity. But missing from that is still a significant part of the defense component, which I think the administration is going to have to focus on next. So our role, I think, is to continue to prod and provide whatever resources are necessary.

Q: Do you feel the issue is getting the legislative attention that is required for that purpose?

Kyl: No. But there hasn't been disagreement in the legislative branch. It's been a bipartisan, bicameral effort. So there's not a problem there. But if you ask — "Is there enough understanding of the issue, either in Congress or in the public generally?" — the answer is "No." And there's not enough understanding or commitment from the administration either.

Q: You alluded to this peripherally, but given the interconnectedness of the information infrastructure, is there a need for the public and private sectors to somehow coordinate their activities on this and work together?

Kyl: Yes, there is. And part of the plan that we anticipate the administration will be developing is to deal with that element of coordination. For example, the Department of Transportation presumably will have a plan that integrates the private sector components of

the transportation industry with the Department of Transportation for joint response — indications and warning and response — and so on. There is also an industry group that's dealt primarily in the telecommunications area that's had a long-term liaison with the president. They continue to give a lot of advice about what the private sector needs, and what they can do to deal with this. Because ultimately, it's the equipment, the technology generated by the private sector that ends up being used by both the private and the government sectors, and they can be pretty innovative about what they build into their systems and how they offer solutions to the government. They've been doing that.

Q: You mentioned earlier a suspicion at one point, which proved to be unfounded, that Iraq was undertaking some activity in the information warfare area. Do you know of any U.S. adversaries that are actively getting into this sort of preparation, and what would be the nature of that?

KYL: According to our intelligence agencies, there are a large number of countries that are working on information warfare techniques, and a smaller number of countries that have specifically targeted the United States in their planning efforts. I cannot say whether there has ever been an attempt by another country to attack our information infrastructure.

Q: I guess the attacks would occur in either of two ways: Actually knocking out certain areas of activity that are controlled by the information system, or by feeding false information into the systems.

KYL: You could go in and acquire information, you could plant various kinds of bugs that would either disrupt or stop operations, or put in false information. So you could really do all three of those things.

Q: And, presumably, somebody somewhere must at least be looking into that sort of effort.

KYL: As I say, there are a large number of countries that have programs under way, some of which are actually aimed at the United States. Now that's to be distinguished from saying that these countries are attempting to attack the United States today; I'm simply saying that they have developed programs, or are in the process of working on the concept of information warfare against the United States. It would also stand to reason, and this may be your next question, that the United States would be thinking in offensive and defensive terms as well.

Q: Could you expand on that a bit?

KYL: The only thing that I would say further is to remind readers that, of course, with respect to the ability to exercise offensive information warfare, we are by far the most vulnerable country because of the degree of our reliance upon technology, so to us it is really more of a defensive thing than an offensive thing.

Q: But you're suggesting that certainly preparations or investigations are under way here as well.

KYL: Well, remember that there was some information that came out shortly after Desert Storm revealing a degree of U.S. disruption of Iraqi communications and other activities which I guess one can say was maybe the first example of the use of information warfare. It's actually not something new. I mean for years, for decades, we've attempted to disrupt the enemy's communications and break their codes and so on — it's all the same thing. This is just a much more sophisticated version of it.

Q: What are you planning within the subcommittee at this point in terms of further activities?

KYL: The next thing we will do is to review the report that's issued in November in response to the Presidential Decision Directive (PDD) which will give us some indication of where the administration is planning to go, evaluate that, perhaps hold a hearing to learn what they're intending there and perhaps hear from people who might have other views, and I'm not sure, at this time, what we will do after that.

Q: Do you see large added infusions of funding being necessary at some point?

KYL: Relatively small actually, but there are going to be some funding requirements, I would say.

GHOSTS IN THE MACHINES?

By Dr. Martin Libicki
Senior Policy Analyst, RAND

The author cites law enforcement as a primary area where global information security can be enhanced. He calls for "the harmonization of national laws against computer attack, multinational cooperation in tracing attacks across national lines, international treaties on extradition of attackers, and a readiness to impose sanctions on those who protect attackers." He believes a willingness to share information on research and development, on attack indications and warnings, and on attack incidents and responses "can also improve the efficacy of each nation's protective measures."

No one looking for something new to worry about need look very far. Everywhere, computers and other digital devices have insinuated themselves into our lives. What was manual is now automated; what was analog is now digital; and what once stood alone is now connected to everything else. Increasingly, we have no choice but to trust them. If they fail, we are sunk.

The faith that dependence breeds would be merited if such devices did only what they were supposed to do. Some do fail on their own, and we go on. But the prospect also exists that they may fail us because they have fallen under the control of those with malign intent. In such circumstances, they may not only go down, but reveal secrets with which they have been entrusted, or produce corrupted information — sometimes in ways beyond notice until it is too late to reverse actions already set in motion.

Why the vulnerability? Digital devices are fast, cheap, accurate, and rarely forget what they are told. But they are frightfully literal and usually lack the discernment to understand the implications of what they are asked to do or the integrity of those who ask them to do it.

The potential consequences of deliberately induced systems failure or corruption are vast. By seizing control of the key systems that undergird society, computer attackers can, in theory, listen to phone calls, misroute connections, and stop phone service entirely; shut down electrical power; get in the way of literally trillions of dollars that change hands every week; hinder emergency services; prevent the U.S. military from responding to crises abroad quickly; reveal personal medical secrets; confuse transportation systems and put travelers at risk; and much more. Life, as we know it, could grind to a halt.

Computer attacks, if sufficiently systematic, may be war by other means — hence "information warfare," as an overarching concept. But information warfare understood broadly — attacking an adversary's information and decision processes — is as old as warfare itself. Such tactics encompass psychological operations, attacks on an enemy's command apparatus, espionage and counter-espionage, and operations against adversary infrastructures and surveillance systems. During the U.S. Civil War (1861-1865) there were incidents of propaganda operations, snipers targeting opposing generals and observers in hot-air balloons, marauders tearing up telegraph lines, cavalry pickets and counter-cavalry demonstrations — all information warfare. World War II saw the advent of electronic warfare in the form of radar, electronic deception, radio-frequency jamming, codemaking, and computer-aided codebreaking.

Computer attacks fit snugly into this continuum of warfare. If one can destroy enemy headquarters with shot and shell, what is wrong with trying less violent means to break into and ruin the computer systems that manage tomorrow's battles? Notions of strategic warfare by 1920 held that using air power against civilian targets would short-circuit the gore of trench warfare. Strategic information warfare goes this one better.

Are modern societies vulnerable? Most information systems have far less security than they could have; many, less than they should have. Networks and

systems of many types have been attacked — Internet service, phone service, some transport services, financial institutions, and corporate networks.

Computer attacks are, by any indication, a serious problem. Indeed, the Federal Bureau of Investigation recently estimated that they cost the American economy somewhere between a half a billion and five billion dollars a year — an estimate with a wide, and, in its way, very telling, margin of error. No one really knows how many attacks take place. Much evidence is anecdotal, and so people have to extrapolate using popular precepts such as, "only amateurs leave fingerprints, professionals never do," and, "people never want to talk about how badly they have been hit." Thus are computer attacks likened to icebergs, with America, supposedly, playing Titanic.

This is the theory, at any rate. But is it a prospect? Unlike virtually all other forms of warfare, there is no forced entry in cyberspace. If hackers enter a system they invariably have done so along paths resident in the system itself: some are features and some are bugs (that is, undocumented features) never removed. Either way, travel along these paths is under the complete control of whoever is running the system. This being so, vigilance suffices for protection.

Indeed, protections exist. Many information systems operate with several layers: there are ways to screen illegitimate from legitimate users, locks to keep legitimate users from taking deliberate or inadvertent control of computer systems, and safety devices so that even the usurpation of control does not create a public hazard.

Attackers, for their part, must first fool a system into thinking they are legitimate users (e.g., by stealing or guessing a password), and second, acquire control privileges (often by exploiting endemic faults) denied to most common users. With such "super-user" privileges, attackers can purge key files, write errant nonsense in others, or plant a backdoor for later reentry.

There is also little doubt that defenses, if need be, could be better than today's common practice.

Most systems use passwords to limit entry, but passwords have many well-known problems: too many are easy to guess; they can be stolen as they flow over networks, and they are too commonly stored in expected places on a server. Cryptographic methods such as digital signatures work around these problems (capturing and replaying access messages does not work). Digital signatures even help ensure that any change to a data base or program, once electronically signed, can be traced to its originator — also useful, if the attacker is an insider entrusted with systems privileges.

Computer and network operating systems are susceptible to hacker-inserted programs such as viruses (software that infects software and causes it to infect other software), Trojan horses (seemingly useful software with hidden traps), and logic bombs (software that lies dormant until signalled). Virus-protection programs may work, but if worries persist, why not put all the critical files on an unalterable medium (e.g., a CD-ROM)? Such a medium can also prevent information from being erased or corrupted by a would-be attacker's digital footprints. Indeed, given the low cost of such devices, there is no legitimate excuse for losing information anymore.

Systems can also be put at risk from other systems they hold to be trustworthy. Two precautions can be taken against this danger: culling the list of trustworthy systems and limiting the number of messages that one's own system will react to. Banking systems, for instance, do this to protect their computers from being corrupted by ATMs (automatic teller machines) sitting on a public street corner. The computer ignores anything from the ATM that is not a legitimate transaction. No legitimate transaction can wreck the bank computer.

A final precaution is to pull the plug. As a last resort, many systems (e.g., nuclear power plants) work almost as well even if unconnected to the outside world.

How far must a system's owners go? Relatively low-cost security protection (e.g., firewalls and intrusion detectors) may seem good enough for the current environment. After all, an office system may not be worth spending great sums of money to protect if, for example, an attack will only disrupt service temporarily. Many companies perceive no serious threat and invest accordingly. They may be right — but what if they are wrong? If and as threats mount, systems owners can increase security — even in the short run (e.g., by

preventing users from logging in from home, or carrying out certain actions if logged on).

Indeed, it is precisely the lack of good security features throughout the national information infrastructure today that leads to some confidence that computer systems could, if necessary, be made safe. (By contrast, good defenses against nuclear warfare were technologically impossible for decades, and, if possible today, are very costly.) Even if many systems can be taken down temporarily, it is another matter to keep them down for a long time while systems administrators work fiendishly to restore essential services. Anyone who would hold the U.S. information infrastructure at risk must realize that the mere threat of doing so — if taken seriously — erodes soon after being announced as people react.

What should the role of government be? Can those responsible for protecting the nation on the ground, on the water, in the air, and in outer space also protect the nation in cyberspace? Should they?

Government can help, but there is much government cannot do — or should not do. Yes, electricity is essential, but protecting its supply from hackers depends almost entirely on how power companies manage their computer systems: this includes the network and operating system software they buy, how such software is configured, how access privileges are awarded and protected, and how the various fail-safe and manual override mechanisms are emplaced throughout the companies' generation and distribution systems. It is inconceivable that any power company would wish the government to "protect" it by telling it how to do these things. More generally, the government cannot build a firewall around the United States — if only because so many internal networks span the globe.

The government can and does enforce laws against computer attacks — and has experienced considerable success considering how anonymous (and faraway) attackers can be. So far, most of the well-publicized hacker attacks that have been detected have been the work of amateurs not professionals.

Should the government try to inhibit information warfare by threatening retaliation against perpetrators? Assume their identity can be established. The U.S. government may threaten like for like, but many rogue states have little in the way of comparable systems (e.g., North Korea lacks a stock market to take down). Conversely, it is problematic to respond violently to an information warfare attack that wasted the victim's time and money, but wounded no one.

While much of what the government can do to enhance security is indirect, the President's Commission on Critical Infrastructure Protection and other entities have made the following recommendations:

— Make sure the government's own systems are protected, because they are important to national security and for setting a standard for others.

— Use research, development, and first-user acquisition to promote the rapid development of security tools.

— Disseminate warnings of impending information warfare attacks (if they can be detected — no small task).

— Promote a legal framework that induces private parties to protect their own systems to the optimal extent.

— Provide a neutral clearinghouse that encourages private parties to collaborate on sharing their experiences and countermeasures on a confidential basis.

By and large, such measures are progressing.

Unfortunately, U.S. government restrictions, extant and threatened, on hard encryption have inhibited one of the better tools for protecting systems and also have reduced the credibility of government actions in the information warfare area.

International Activities: Extending most of these government actions overseas suggests an opening agenda for guiding international activities against information warfare.

Law enforcement is a big area. The harmonization of national laws against computer attack, multinational cooperation in tracing attacks across national lines, international treaties on extradition of attackers, and a readiness to impose sanctions on those who protect attackers can all aid global information security.

A readiness to share information on research and development, on attack indications and warnings, as well as attack incidents and responses can also improve the efficacy of each nation's protective measures. However these areas are often the province of intelligence agencies, not historically noted for transparency in such matters.

Conclusions and Harbingers: In the post-Cold War world, there is an increase in new and unconventional threats (e.g., nuclear-armed terrorists) which are scary, but, as yet, notional. Information warfare is among them. The more that information systems pervade society — its defenses, commerce, and day-to-day life — the more their well-being matters to us all. The potential for major mischief does exist, particularly if undertaken in a systematic way by a well-financed adversary. But what is also striking is the fact that even though information warfare is relatively inexpensive, so far, there has been a paucity of really damaging incidents.

Two indicators may reveal a great deal about the true risk from systems attack. One is how people react to the year 2000 computer problem. Assume a large share of the world's information systems crash at midnight on December 31, 1999. Will panic and paralysis result, or will people quickly find ways of working around the problem or doing without information for awhile? If lawsuits erupt, what precedents will be established to assign responsibility to people for harm done if their systems fail?

The other harbinger is of more recent origin. Were one to imagine the most plausible perpetrator of serious information warfare terrorism, it would be someone with nothing that can be held at risk (i.e., not a country), several hundred million dollars in hidden cash, an appreciation of technology, an international network of nefarious friends, and a vicious score (real or imagined) to settle with the United States or some other nation. Sound familiar? If it does, what happens in the next year may reveal whether powerful individuals or groups might try to bring a country to its knees through information warfare — or whether they direct their efforts elsewhere.

THE RESPONSE OF HIGHER EDUCATION TO INFORMATION WARFARE

By Dr. Charles W. Reynolds
Director, Department of Computer Science, and
Interim Dean, College of Integrated Science and Technology
James Madison University

There is a growing demand for information security professionals in an era when "malicious vandalism, criminal activity, and international information warfare" all may threaten the nation's information infrastructure, says Dr. Charles Reynolds. He describes how the academic community is collaborating with government and industry to meet that need through an initiative launched in 1997 called the National Colloquium for Information Systems Security Education (NCISSE). The author, 1998 chairman of NCISSE's executive committee, also outlines James Madison University's efforts to respond to emerging national priorities in countering the threats to U.S. information networks.

THE NEED FOR INFORMATION AND COMMUNICATION INFRASTRUCTURE PROTECTION

All aspects of our lives and all aspects of our social, economic, and political systems are becoming increasingly dependent on our information and communications infrastructure. Our financial systems, our transportation systems, our water and electrical utilities, and all other critical infrastructures have become dependent on our information and communications infrastructure. Yet this infrastructure is the most vulnerable of all our infrastructures to malicious vandalism, criminal activity, and international information warfare — all of which may threaten it and so threaten all other infrastructures that are dependent on it. The security and assurance of our information and communication infrastructure is therefore a national priority.

To counter the threats of the new era in information technology, our nation needs an information-literate work force that is aware of the emerging vulnerabilities of critical infrastructures, as well as a cadre of information security professionals who are knowledgeable about the recognized "best practices" available in information security and information assurance.

A NATIONAL DIALOG WITH HIGHER EDUCATION

In response to the need to protect the nation's critical infrastructures, the National Colloquium for Information Systems Security Education (NCISSE) was created in May, 1997, to provide a forum for dialog among key figures in government, industry, and academia on ways to work in partnership to define current and emerging requirements for information security education. NCISSE also seeks to influence and encourage the development and expansion of information security curricula, especially at the graduate and undergraduate levels.

At its second annual meeting in June, 1998, at James Madison University in Harrisonburg, Virginia, the Colloquium agreed that NCISSE would strive to foster development of academic curricula that recognizes the needs expressed by government and industry, and is based on recognized "best practices" available in the field.

The Colloquium's goals also focus on the need to assist educational institutions by fostering the continued development and sharing of information security education resources. NCISSE encourages educational institutions to teach appropriate information systems security courses in various curricula to meet the needs of 21st century consumers and to offer courses to meet the growing demand for information systems security professionals.

At its 1998 annual meeting, the NCISSE issued a wide-ranging agenda for action by its various constituents. These included tasks for government, industry, and institutions of higher education to undertake both individually and in cooperation with each other.

Especially important among the joint actions needed is clarification of the knowledge, skills, and attitudes that define an information security professional and thus develop standards for what information security professionals should know and be able to do. Because information security is itself still coalescing as a body of knowledge, we need to identify current "best practices" for inclusion in professional standards in a way that can continue to evolve. Finally, all three constituents of the Colloquium must overcome the resistance among information security personnel to standards because it is adherence to the discipline embodied in standards that is expected of any profession.

Also outlining recommended actions for private industry, the Colloquium said the industrial sector should provide educational institutions with funding, equipment, and software, and help with the maintenance of computer systems on university campuses; provide on-site training for university faculty, including those who have not previously worked in information security; and fund internships for students to work in the information security area.

The NCISSE urged government to develop and share course work in information security and to encourage the development of university Centers on Infrastructure Protection modeled after the Materials Centers sponsored by the National Science Foundation and the Transportation Centers sponsored by the Department of Transportation.

Colloquium members called on information security professionals throughout the nation to improve networking among faculty, sponsor more conferences on information security, launch more Web sites, and publish more journals related to the protection of U.S. information networks. They also underscored the need to establish a formal system of recognition for outstanding educational programs in information security.

Focusing on institutions of higher education, the NCISSE encouraged educational institutions to increase programs with concentrations in information security and include security courses in core curricula of all college graduates.

Especially important is the inclusion of curricula that address the ethical and cultural issues that arise in modern information systems. Questions here include both how traditional values are preserved in the modern information era and how they may need to change.

Since many ethical and cultural values are formed early in life, institutions of higher education are encouraged to develop information security curricula for and in collaboration with secondary education.

In recognition that higher education is itself a profession guided by standards, educational institutions were encouraged to solicit guidance from accreditation organizations for appropriate placement of information security within their curricula.

Finally, because education is a life-long concern in a rapidly evolving technological society, higher education was encouraged to provide continuing educational programs for information security professionals who are already working in the field.

The Colloquium recommended that information security educators develop and share practical laboratory exercises in information security, design computer games that express appropriate values for a responsible and information literate work force, develop a place to share instructional materials, and write more textbooks, especially on practical issues.

The NCISSE's agenda for action also called on specialists in legal education to help U.S. lawyers understand information security.

INTERNET-BASED INSTRUCTIONAL METHODS

The national critical need for information security professionals is typical of the modern technological world. As technology changes rapidly, professionals must be committed to life-long learning that constantly renews and extends their skills. And all professionals must be prepared to reorient their careers and acquire new skills as changing technology drives changing work-force needs.

The need for information security professionals has mushroomed in recent years. This demand for skilled professionals, in turn, has generated demand for educational opportunities that supply new professionals and reorient current professionals in a new direction. Yet, it is unreasonable to expect that these professionals

seeking continuing education will interrupt their current careers and family life to attend a traditional on-campus university. It is for this reason — the need for ongoing education for adult professionals that does not interrupt their careers or family life — that there is so much interest in Internet-based education. James Madison University has responded to this need and to Internet technology with an Internet-based graduate professional program in information security.

The curriculum is offered as an Internet-based learning program through contracts with organizations that can ensure the integrity of the testing procedures for their employees.

The program is structured in 13 courses of seven weeks each and spans slightly more than two years. A group of students called a "cohort" enter the program together and complete all 13 courses together in sequence.

The Internet-based learning program combines independent study with guided instruction and group collaboration that are coordinated by a central facility that provides a network of services. Professors and technology provide a delivery system that maintains high academic standards while being flexible and considerate of participants' needs. Electronic discussion groups examine, discuss, and critically evaluate information security concepts. Each course consists of a sequence of readings and problems to be solved.

Internet presentations of concepts can be viewed on any Internet workstation from anywhere in the world at any time. Projects in each class offer practical orientation to concepts and materials learned.

THE INFORMATION SECURITY PROGRAM AT JAMES MADISON UNIVERSITY

Participants who complete the Information Security Program at James Madison University earn a master of science degree in computer science with a concentration in information security. The program is based on a standard endorsed by the National Security Agency and is designed to develop the knowledge and skills necessary to understand the interrelationships between information security and information technology and to relate both the technical and human components of information security and information technology.

The basis for the courses conducted by James Madison University faculty centers on the administration, management, evaluation, and implementation of computer technology with emphasis on information security. The management of information security programs includes the preservation and protection of information confidentiality, integrity, availability, authenticity, and utility within acceptable limits of risk.

The program members, working in teams:

— Develop the knowledge and skills necessary to understand the relationship between information security and advancing the information systems technologies needed to implement crime protection and detection programs;

— Develop advanced competencies associated with technical, supervisory, policy, and related positions in information security and computer technology with regard to vulnerabilities, threat, and risk assessment;

— Gain perspectives required of effective information security analysts, managers, administrators, and practitioners in planning, evaluating, and implementing information security techniques and programs;

— Relate the technical and human components of information security and computer technology in the protection of information systems;

— Develop core competencies in data-base and information systems design, in operating systems and networks, and in application software development to enhance crime prevention and investigation responsibilities.

The program begins with a preparatory segment for those who need to strengthen their computing skills before beginning the computer science core. This is followed by three courses in computer science that cover data-base management, operating systems and networks, and application software development. Building on this strong foundation, the third period introduces information security, the concepts of trusted information systems, and techniques for secure information storage and transmission, especially by encryption. The fourth segment teaches management and administrative issues in information security including risk and

vulnerability analysis, information system audit tools and procedures, and legal, ethical, and policy issues. A final capstone project integrates the whole program with a project that challenges participants to analyze the security of an information system.

THE INFORMATION SECURITY CURRICULUM AT JAMES MADISON UNIVERSITY

The information security program at James Madison University includes the following courses organized into segments:

1. Computer Science Core Segment

Operating Systems and Networks — Concepts and principles of multiple user operating systems. Memory, CPU (central processing unit), I/O (input/output) device allocation, scheduling, and security. Memory hierarchies, performance evaluation, analytic models, simulation, concurrent programming, and parallel processors.

Data-base Management Systems — Types of physical storage and access methods; data models; relational algebra and calculus, and definition and query languages; dependencies, decomposition, and normalization; data-base design; recovery; consistency and concurrency; distributed data bases. Examples from commercial data bases.

Application Software Development — The software development life cycle, software project management, development tools and methods, software quality assurance, programming language paradigms and their use in software development.

2. Information Security Technical Segment

Introduction to Information Security — Overview of threats to the security of information systems, responsibilities, and basic tools for information security, and for the areas of training and emphasis needed in organizations to reach and maintain a state of acceptable security.

Trusted Systems — Definition of a "Trusted System," and considerations pertaining to the design, evaluation, certification and accreditation of trusted systems, including hardware considerations, software considerations such as developmental controls, validation/verification, assured distribution and other assurance issues. Implementation, configuration management, and systems administration of trusted systems. Importance of understanding the psychology and the successful modus vivendi of the attacker to generating and maintaining a powerful defense.

Cryptography — This course provides the student with an understanding and the ability to implement major encryption protocols. It deals with the design and analysis of systems that provide protection for communications or resist cryptographic analysis.

3. Information Security Management Segment

Information Systems Vulnerability, Risk, and Analysis — Vulnerabilities and risks inherent in the operation and administration of information systems are identified and explored.

Information Security Audit Controls — Students develop plans and conduct an information security audit to include an in-depth physical security survey. They develop and implement standards for monitoring the normal activities of an information system.

Policy, Procedures, Legal Issues, and Ethics — Development, evaluation, and implementation of administrative security policies and procedures in a UNIX system in a secure environment. Preparation of a Security Administrative Guide or an annex for such a document.

4. Information Security Capstone Project

A final capstone project integrates the whole program with a project that challenges participants to analyze the security of an information system, to survey and analyze the effectiveness of available options for enhancing that security, to review the broader legal and ethical context of those options, and to select and propose an implementation procedure for one of the options.

Preparatory Classes — Students not ready to begin the core segments may enroll in a preparatory sequence of three classes: Accelerated Fundamentals of Computer Programming, Advanced Fundamentals of Computer Programming, and Accelerated Fundamentals of Computer Systems.

PRIVATE, PUBLIC SECTORS BENEFIT BY SHARING EXPERTISE ON SECURITY

An interview with Howard Schmidt
Director, Information Security, Microsoft Corporation

Government agencies and many private corporations now have the ability "to contact each other and support each other" in the event of threats against their information and other critical systems, says Howard Schmidt, Director of Information Security for Microsoft Corporation. He also cites extensive cooperation among corporations to deal with information warfare questions. "When it comes to security issues, there are very few things that relate to competition," says Schmidt. "We work with our competitors and partners alike to assist in standard developments so that we can all succeed in developing and maintaining good security." Schmidt was interviewed by Managing Editor Dian McDonald.

Question: How do you assess the vulnerability of U.S. critical infrastructures to cyber attack? How prepared is the U.S. to withstand such attacks?

Schmidt: My assessment is pretty consistent with that of the Presidential Commission on Critical Infrastructure Protection: We've got some work to do. These were issues that, as this was being established, were not really at the forefront. As far as our ability to withstand such attacks, I think the President's Commission on Critical Infrastructure Protection has gone a long way to bring together the private and public sectors to be able collectively to withstand these types of attacks and basically do a pretty good job of responding to them.

Q: Have you worked with the commission?

Schmidt: Yes, we have worked with the commission. We have had them out here (in Redmond, Washington) for a couple of meetings. I have been back to Washington, D.C., for a couple of meetings. And, as a matter of fact, we are putting together a pretty good sized meeting of folks from the government and the private sector, bringing them together to reach agreement on ways to make a better infrastructure.

Q: What organizational changes has your company made as a result of the new threats to technology?

Schmidt: Let me rephrase that question, if I could, because we are not looking at it as threats to the technology. We are looking at it as the use of technology to give somebody an opportunity to go ahead and do something against a larger audience, so to speak. Basically what we are seeing is: the same old types of threats are there, but they are using the newer technology.

In response to that, we created one year ago a program that we are very proud of: the MIAP or the Microsoft Information Assurance Program, which gives us the ability to tie together a lot of the interests internally that would be relative to protecting our information or assuring that our information is valid. We now have under one organizational "umbrella" various programs and functions including our disaster recovery plan, our data retention and classification system, our backup strategy, the information security group itself, the physical security group as it relates to information assurance, as well as the product security group since Microsoft is a software developer.

Under this structure we have the cross-feed and cross-utilization of all the specialties, not only to secure our information and systems, but to make sure that the products that we are working on have the benefit of the experience of those who are in the information security field to help make them better.

Q: In terms of strategies to deal with information warfare, to what extent are you working in concert with other corporations?

Schmidt: Very much so. As a matter of fact, we have a number of different groups: for example, the Information Systems Security Association, which is a non-profit

organization whose members are involved in the security field — for example, representatives of Charles Schwab Company, U.S. Space Alliance, Air Touch Cellular, and different government agencies. We participate in conferences, and we work with the Gartner Group, a big computer consulting firm. We are participants in the initiative of former Senator Sam Nunn, who has been very instrumental in the infrastructure protection arena. He coordinates a recurring security forum down at Georgia Institute of Technology in Atlanta, and we have been a part of that forum as well.

So there is a lot of cross-feed of information, best practices among us in the security field in the private sector. And there are other groups, such as the Federal Computer Investigations Committee and the High Tech Crimes Investigators' Association, that are comprised of both public and private sector representatives who work together in this area. So we've got some really good relationships, and we work very closely together.

When it comes to security issues, there are very few things that relate to competition. We work with our competitors and partners alike, to assist in standard developments so that we can all succeed in developing and maintaining good security.

Q: Can you elaborate on how your organization is working with the government sector in meeting the new challenges to information systems?

Schmidt: We have a couple of different avenues. Of course the product folks who create the products that we all use have very, very close ties with the government workers in all the government agencies to make sure that the products are being built to meet the needs of government in securing the critical infrastructure.

On the other side of it, as an online service provider, we are as well part of the infrastructure ourselves, and we work very closely, for example, to provide technical expertise to assist those individuals who conduct online investigations. We now have a "24 by 7" (24 hours a day, 7 days a week) hotline number for the law enforcement community as it relates to investigations of people doing things illegally on the Internet.

Also we have recurring best practices meetings. We do a lot of presentations at government meetings. For example, I delivered a keynote speech at the National Defense University in Washington, D.C., a few months back. I was at the "Defending CyberSpace '98 Conference" in D.C. in September. We participate in those types of forums, sharing our mutual experiences to the betterment of all of us in the field.

Q: Do you believe that the government should play a more prominent role in protecting critical infrastructures, and, if so, what could that role be in your view?

Schmidt: Basically, I believe that the government should continue in the role of working together with the private sector. I think that Presidential Decision Directive 63 (PDD 63), which established the Critical Information Assurance Office, really lays out a good framework for putting the government in a good position to work with the private sector. And I think that with that governmental role — and without new legislation or new rules or regulations — we can go a lot further to work with the government to make sure that critical infrastructures indeed remain a protected resource.

Q: Do you see clashes of philosophy in the United States between corporate information requirements and government security concerns?

Schmidt: Basically I don't see a clash. I think what we see in that vein is that we all are looking to make sure that we have maximum security while protecting the privacy of our corporate information, government information, personal information, and things of that nature. So even though there may be some differences in terms of how we approach the issues, I think the critical point is the fact that we all agree that we need to work collaboratively to ensure that the infrastructure is protected.

Q: How can the public and private sectors work together better to develop effective defensive capabilities against terrorist or other hostile action?

Schmidt: I think I have pretty much addressed that, but the bottom line is: we now have with various government agencies and a lot of the different corporations the ability to contact each other and support each other in the event that anything like this should take place. And I think we are in pretty good

shape when it comes to providing technical expertise to law enforcement support groups. Obviously, we are still working out some of the ways to institutionalize and formalize these procedures more, but I see us doing that now and continuing to do it and do it better.

Q: How does Microsoft build security into its products to help customers protect themselves?

SCHMIDT: That is something that is kind of beyond my area of responsibility, but what I can say is that Microsoft representatives meet regularly with their customers. We all have concerns about security. Microsoft's product development employees constantly are working to ensure that all of their products are more secure, and they work with us and the information security professionals because we run our own products up here. So there is constant feedback, making sure that the products are as secure as they can be now — and in the future, as more vulnerabilities may be discovered out there.

Q: Do you believe that with current technological controls, protection is now possible against computer viruses and cyberterrorists?

SCHMIDT: There has been a lot of publicity recently about different viruses and other things that are out there. Obviously, it's just like any other type of illicit activity as these things are discovered. We, in the private sector and government, work collectively to counter them and to make sure that we stay ahead of such threats, as well as look to the future to try to predict what somebody might try to do. As long as we have the sharing of information and the great information systems that we all rely on, there will be people who will try to do something against those systems. But the bottom line is: with technology and human education and awareness of the risks, I think we can do a pretty good job of handling any of the protective issues related to them.

Q: Have you developed technology that could protect a company from an unrelenting deluge of e-mail messages from a cyberterrorist?

SCHMIDT: Yes. There are a number of resources built in and a number of updates and patches that we have put on our products and that other companies have put on their products to alleviate this sort of a problem. Also, there are some companies that we work with in our Security Partners Program that have developed some really, really good tools — by tools, I mean computer programs — that would really help to protect against denial of service attacks and e-mail bombs and things of that nature. We have come a long way in fixing that problem.

STRATEGIES FOR COUNTERING THREATS TO INFORMATION TECHNOLOGY ASSETS

By James A. Lingerfelt
Senior Consultant, IBM, Public Safety and Justice

The primary threat to information systems is not the evil super hacker, says Lingerfelt, an expert in technology and strategic planning in law enforcement. "Rather, the greatest dangers to computer systems and data bases are 'trusted' sources." The author emphasizes that "a realistic assessment of security needs and threats, followed by meaningful formulation and implementation of a security plan, can provide effective protection against the vast majority of threats, and at a reasonable cost." He identifies areas that are the most frequent sources of real threats and provides seven basic strategies for planning information technology security.

Law enforcement and criminal justice agencies have an unprecedented opportunity to use information technology (IT) to transform their operations and to provide better, more effective service. However, many agencies are reluctant to pursue the opportunity because they fear that by replacing or supplementing their closed mainframe systems with networked PCs, and implementing automated reports and computer networks, they would expose themselves to attacks by hackers. The high estimated costs of protecting an entire IT system against penetration by super hackers, combined with the damage that could result from the loss of extremely sensitive information, make avoiding the (perceived) risk altogether seem reasonable, despite the gains to be achieved by the use of IT.

It is a fact that because of exponential increases in the use of IT, there is an increased exposure to attacks on information systems, assets, and data bases. However, the feared super knowledgeable computer hacker is rarely the biggest threat. Rather, the greatest dangers to computer systems and data bases are "trusted" sources who often operate in the absence of even minimal attention by police and criminal justice agencies to basic IT security. A realistic assessment of security needs and threats, followed by meaningful formulation and implementation of a security plan, can provide effective protection against the vast majority of threats, and at a reasonable cost.

PERCEPTION VERSUS FACTS

Many departments have made substantial financial commitments to IT. This has been accompanied by an increase in the number of reports of hacker attacks against police information systems.

There are also increased reports of illegal use of information from police data bases, thefts of police information, and thefts of IT assets belonging to police agencies. The frequency of these reports has discouraged many police agencies from venturing beyond their existing closed systems. However, new business requirements imposed on criminal justice agencies demand that they change the methods by which they acquire, share, and disseminate information.

Operational changes have been initiated as a result of the need to distribute information systems to the field, streamline work processes, distribute information beyond organizational boundaries, or to exchange information with outside agencies and individuals.

Some agencies have responded by using personnel to perform the new duties, thus drawing from the available field force. Others have implemented new "stand alone" systems that provide only the new services, but are not integrated with or complementary to the agency's legacy systems. This only increases the complexity and costs — in people, time, and money — of supporting IT.

As already noted, internal threats from sources within the trusted domain cause more damage than intruders. Several incidents caused by internal sources have been documented:

— An entire department's network was brought down by a virus on diskettes that the department's planning division distributed to collect survey information.

— The chief of intelligence overseeing a hierarchical intelligence system taped to his monitor his user ID and password with detailed log-in instructions.

— A senior official of a police department sold to organized crime representatives a file containing the description and tags of all undercover cars used by police officers.

— A novice network administrator setting up a network at a police department gave every user administrator privileges.

— Applications programmers at a major police department were allowed to put a new program code directly into production without methodical testing and review, and the entire system was brought down for 24 hours as the result of the bad code.

— A state government set up a web site with no firewalls. Within 24 hours, its user ID and password file were posted on a hacker conference. To the state's credit, it shared the experience with other states and thus helped them avoid the same mistake.

Not one of these stories involves a super hacker successfully attacking an agency information system. The last example was a penetration made possible by the worst possible open door. All of the incidents could have been prevented by some basic planning, training, and oversight.

In sum, there is an increased threat of external attack as a result of the increased use of information technology, but the proportionate threat as a piece of the total pie has not changed — it's just a bigger pie. Increased threat? Yes. Different threat? No.

The increased exposure to computer security threats is due to several causes:

— New business models: The public sector is mirroring the private sector, with a delay of about five years.

— Exponential growth in use of IT: Computers and networks have insinuated themselves into almost every part of our lives.

— Reduced costs: Today's technology is inexpensive. Regardless of the metric that is used, costs for basic IT are lower than they have ever been, and the cost of new technology is decreasing faster than it did only a few years ago because of the rapid advances and increased competition.

NEW BUSINESS MODELS

In the transition from centralized to dispersed operations, the headquarters as center of the decision-making and information universe has been replaced by remote independent business units supported by distributed IT.

In IT this shift has meant transition from closed architectures to networks — intranets and extranets. The distribution of information means more difficulty in protecting assets, monitoring operations, and responding to problems. There are more points of exposure. The good news is that distribution of IT is making huge gains in productivity possible — with return on investment often occurring in less than one year.

Private sector organizations have begun to focus on core competencies instead of trying to provide all things to all people. Businesses are maintaining much smaller personnel rosters. This allows them to avoid labor problems and logistical problems associated with changes. Only positions that contribute directly to achieving business goals are staffed. Mergers and acquisitions frequently call for outsourcing to deal with support and administrative functions, particularly IT. Criminal justice agencies (and all of government) have begun moving in the same direction to streamline operations, reduce costs, and improve services.

Additionally, retention of good IT personnel has become very difficult. Governments have not been able to compete with private sector salaries to replace lost personnel. This also has increased the use of outsourcing in government.

Increased turnover of executives and managers is another fact of life in organizations today. As companies downsize, or as they raid each other for talent, there is a

threat of executives or middle managers taking important intellectual property with them. One such case was successfully prosecuted when the directory structure of a manager's computer files was shown to be identical to that of his previous business unit. Rarely acknowledged or published is the fact that companies that downsize often lose millions of dollars in stolen hardware, software, supplies, and furnishings if employees are given advance notice.

Despite the benefits, outsourcing IT can result in security exposures. A security plan is especially important when mission-critical IT responsibilities will be turned over to contract employees or agency outsiders. The agency may require that certain background investigation requirements be met by all contract employees.

EXPONENTIAL GROWTH IN USE OF INFORMATION TECHNOLOGY

Computers and networks have insinuated themselves into almost every part of our lives. Fraud, theft, and dissemination of illegal information and materials are made possible by the computers, networks, and Internet we all use. New kinds of crime are devised and old schemes are given new life.

Fortunately this growth in computer use has produced advances in technology, standards, and identification of best practices. As the lessons of mistakes have improved the technology, we have all benefited. Security practices have also improved in direct response to lessons learned, and a solid set of best practices has emerged. The private sector has paved the path. Most new products (hardware and software) have security functionality designed into them. Whether the functions are used is a different matter.

REDUCED COSTS

Regardless of what metric is used, the costs for basic IT are lower than ever. Almost anybody can afford a computer.

Not only does IT cost less, more money is available for IT investment in the public sector than at anytime since the late 1960s and early 1970s. For example, initiatives related to the year 2000 computer problem and to computer crime are providing billions of dollars for the express purpose of upgrading or replacing public sector information systems. This creates a perfect opportunity for criminal justice agencies to include security in the development and implementation of new business processes and IT systems. Trying to retrofit security is too expensive, and it usually doesn't work.

INFORMATION TECHNOLOGY PLANNING

The science fiction book "Hitchhikers Guide to the Galaxy" has as its first rule:

DON'T PANIC. This is good advice for IT security planning, too. Many organizations have resisted investing in IT because of the persistent and exaggerated belief that they will immediately be besieged by hackers and intruders.

Despite the increased exposure and the increased number of potential intruders, the experience and the tools to build effective defenses are already available and improving all the time. With effective advance planning, it is possible to respond rapidly and appropriately to any attack, preventing most and minimizing the impact of the rest.

Overall IT planning must be done with the big picture in mind: the IT plan should flow directly from the organization's operational plans. The plan should describe business requirements that will fulfill operational goals: it is not an IT wish list. Focus on what needs to be done, not on how it will be done. There are usually many ways to meet a requirement with big differences in cost. There should be a clear justification for every dollar spent. And security must be built into the IT plan from the beginning.

Architectures should be kept simple. This provides a major security advantage. Multiple systems, regardless of how tightly integrated, offer multiple points of access and require multiple security administration and support systems which translate into increased costs.

SEVEN STRATEGIES TO ENSURE INFORMATION TECHNOLOGY SECURITY

1. ABOVE ALL — KEEP IT SIMPLE. If the system is too complicated, users will avoid it or try to circumvent it, thus defeating security and reducing its usefulness. Modern security measures can be effective and unobtrusive.

2. DEVELOP POLICIES, PROCEDURES, AND PENALTIES (P3) IN ADVANCE. Design security P3 that are based on user needs, the nature of the applications, and the information being secured. ENFORCE THEM consistently. P3 without teeth are worse than having none.

3. PROVIDE TRAINING IN THE USE OF THE SYSTEM AND EMPHASIZE THE P3. Reinforce training by reviewing and distributing relevant news items — for example, stories related to cyber attacks or abuses of systems.

4. USE AVAILABLE "OFF-THE-SHELF" SECURITY PRODUCTS AS MUCH AS POSSIBLE, RATHER THAN DEVELOPING SECURITY APPLICATIONS INTERNALLY. This is advisable for several reasons because business needs are relatively straightforward. Criminal justice agencies associate people with other people and people with events, by collecting and sharing information. Standard products based on open standards have been tested and proven, and their customers can be interviewed and learned from. Even if the products are new, the methodologies used in testing can be evaluated and the results reviewed. Most importantly, standard industry products are typically well-documented for users and for IT technical staff. Documentation and testing for security are frequently neglected when applications are developed in-house.

5. COMPARTMENTALIZE INFORMATION, ASSETS AND USERS. PROTECT INFORMATION AND ASSETS APPROPRIATELY ACCORDING TO THEIR VALUE. Confidential intelligence reports should be highly secured. Information that is public and/or easily replaced, however, does not require elaborate security. An objective assessment of information assets will show there is substantially more of the public than the confidential.

Similarly, IT assets (PCs, servers, cables, hubs, etc.) and supplies (software, diskettes, etc.) should be appropriately inventoried and secured. Frequently, agencies receive large amounts of hardware and software (PCs, monitors, network cards, hubs, routers, etc.) without entering the items into an asset control data base, and without checking them carefully to ensure they are what was ordered and that the items are configured correctly and work properly. When items are lost or fail to perform properly, there is no record to prove the loss or that the system is not performing as required. Inventory management is a first step. The second is configuration control.

At the time of delivery, the configuration of every piece of hardware should be set and every piece of software should be properly registered. The inventory will then contain a detailed description of every system's components, hardware, and software and where they are located (right down to the office number and desktop). This information is invaluable in protecting assets, identifying theft or tampering, and conducting effective investigations when problems are detected. Software programs are available that check configuration and report problems to security administrators automatically. These programs also maintain a log of changes or maintenance of the system. As repairs or upgrades are made to systems and maintenance is performed, it is important that such activities are logged. Finally, locks and specialized screws to seal workstations can reduce theft or tampering. Policy should require that all suspected problems be reported for investigation.

Compartmentalizing supplies and assets means treating them more appropriately according to their cost or importance to the mission. Often this area is neglected. For example, agencies lock up inexpensive supplies such as diskettes while critical assets such as a server are unprotected in an open office area, and network cable and hubs run across open walls instead of being encased in conduits and hidden in ceilings.

Compartmentalize users as well. Control the applications and information users have access to and how they can access it. (For example, a user may be permitted to access a restricted file only from certain workstations and at certain times). Control who can create accounts or user IDs on a system. Audit these frequently for dummy IDs or accounts.

Have good audit capabilities in place.

One of the most frequently overlooked security threats relates to system documentation. Documentation of all types is often treated too casually and can be found lying open in unsecured offices. Detailed technical and user information must be protected. It may seem convenient and less expensive to prepare and publish "one size fits all" documentation, but it can be

dangerous to system security. Widely distributed end user manuals often contain large amounts of technical information that is useless to the end user, but is very valuable to a hacker. A hacker armed with detailed system information can attack a system with surgical accuracy instead of resorting to more easily detectable brute force attacks. Distribute documentation on a "need-to-know" basis.

Secure documentation, control access to it, and train users how to protect it. Publishing documentation on the network instead of in printed documents is recommended to reduce costs, simplify updates, and provide more protection.

6. BE REALISTIC ABOUT SECURITY ADMINISTRATION. It is not likely that criminal justice agencies, for example, can set up or administer an impenetrable IT security program. Balance realistic security needs against the costs of security. It may be possible to hire the desired level of support to accomplish the same goals. Use in-house staff to do what they realistically can do effectively, and outsource or "resource" the rest. The key is to achieve the results defined by the information security plan.

Many resources are available to meet security needs. They can be outsourced to a private company at competitive costs. As reliance on IT increases and security becomes a greater concern, business is responding by offering high quality IT security services.

There is also value in "resourcing." Resourcing describes what criminal justice agencies and members of the security community can do for each other. Sharing resources, pooling money for joint acquisitions, donated services from universities or from the community — all are potential ways to close gaps in the security plan.

7. TEST, AUDIT, INSPECT SITES AND INVESTIGATE CONTINUOUSLY AND RANDOMLY. Use a methodology for reviewing and testing code to block back doors into systems. Use automated audit and monitor programs. Use programs that check for changes to a file. Develop and use "Tip" programs as a way of identifying existing or would-be systems attackers. Publicize threats and responses to them. Always take swift, consistent, and appropriate action when violations are detected or reported. Announce disciplinary actions taken in IT security cases widely.

EMERGING TECHNOLOGIES

IT security has advanced as rapidly as every other aspect of IT, but it cannot be effective if it is not properly deployed. Security features are available in almost every commercial off-the-shelf application. Firewalls are more powerful and adaptable than ever and are very reasonably priced. Encryption programs are becoming more powerful and easier to implement and maintain. The ability to manage and monitor distributed systems from a single point in the network is improving steadily. Automated monitoring and audit programs to control system use and alert security administrators to attempted abuses are maturing rapidly.

One of the areas of technical advance that is most promising is biometrics — the ability to identify someone based on a unique physical characteristic (for example, fingerprint, voice, hand geometry, retinal pattern, etc.). Biometric devices make it possible to authenticate users more effectively than ever and will prevent unauthorized persons from accessing a system even if they possess a password.

IBM, in cooperation with Barclays Bank in Europe, is piloting workstation keyboards with an embedded fingerprint reader. The users must be biometrically authenticated before they are allowed access to any part of the system. Flash technology (a search algorithm for images) is fast and accurate. It can search a data base of millions of records (including fingerprint images) to determine whether there is a match. This capability, combined with high speed networks, has great potential for use in ATMs (bank automatic teller machines) and other electronic transaction devices. Flash technology is being used for a fingerprint-based voter registration verification system in Peru. The project has had excellent results and will help prevent voter fraud.

As these technologies continue to evolve, IT security will continue to improve in terms of effectiveness and ease of use.

INFORMATION WARFARE: CHALLENGE AND OPPORTUNITY

By James Adams
Chief Executive Officer, Infrastructure Defense, Inc.

"I have the power, the capability, sitting in my home with my computer and my modem...to wage war," says James Adams. "That is a very different environment than anything that we have experienced in the past." Adams is Chief Executive Officer of Infrastructure Defense, Inc., which provides a forum for exchange of information and decision making on the critical infrastructure within the private sector and between the private and public sectors worldwide. This article is adapted from comments by Adams at the U.S. Information Agency in August 1998.

The U.S. military last year organized an exercise that involved a simulation in which an international crisis was brewing and a foreign government had hired 35 computer hackers to disrupt the United States' response to that crisis. The "hackers" taking part in the exercise — called Eligible Receiver — were, in fact, U.S. government employees. They were given no advance intelligence. They bought their laptops from a local computer store.

The hackers successfully demonstrated that they could with ease break into the power grids of all the major U.S. cities — from Los Angeles to Chicago to Washington, D.C., to New York — that were linked to the U.S. capability to deploy forces. At the same time they were able to break into the "911" emergency telephone system and could comfortably have taken both of those networks down.

They then moved on to the command and control system of the Pentagon. Over the course of a few days they interrogated 40,000 networks and got root-level access to 36 of them. They were able to go deep inside the command and control structure and, if they had so wished, could have prevented that structure from working effectively.

What this exercise demonstrated was that 35 people using publicly available information with skills that were available around the world really could have prevented the United States from responding to the crisis.

That is an extraordinary demonstration of the power that information warfare represents. That power has impelled the United States to invest very large sums of money in developing an effective offensive capability where war can be waged by other means.

For those who have the capability, there is the opportunity to wage war — not by deploying soldiers in a conventional sense on a battlefield, with many thousands dying, or, indeed, even deploying missiles in the conventional way — but instead launching through cyberspace bits and bytes that can effectively destroy a potential aggressor before the troops meet each other on the battlefield.

This means turning out the lights in a major city. It means preventing the foreign exchange market from operating properly. It means interrupting the information flow in a foreign country and inserting one's own information flow to make it possible to wage very effective psychological operations against a potential enemy.

These things sound quite mild but, in fact, they can cause the kind of loss of life that a very large bombing campaign might equally achieve.

For example, a study by the U.S. Air Force on the consequences of taking out the Southwestern power grid in the United States showed that 20,000 people would have died. That would have a devastating effect on the morale of the country and present very interesting new challenges of how we respond.

In the drama with Iraq a few months ago, as we scaled up to take possible military action, there was an effort detected to interfere with the U.S. logistics network.

The source of the effort eventually was tracked down to a building in Abu Dhabi. The assumption was that this was Iraqi leader Saddam Hussein waging information war against the United States in advance of the military action. Americans were deployed to deal with this threat. After they reached the relevant building, they discovered a router (transfer point) on the Internet and, in fact, that the "attack" was being launched by some teenagers in the United States.

That is an absolute illustration of the real challenge and opportunity that information warfare represents. We can launch an attack, and it can appear as if it came from somewhere far distant from its actual point of origin. Likewise, when an attack is launched against us, it's very, very difficult to discover where that attack came from. Even if you can discover the source, it's very difficult then to launch a strike. What are you striking and why are you doing so? What public response, public support, will there be for the actions that you are taking if thousands of people die? How do you actually persuade people that this was the right thing to do? There is no evidence to cite of dead babies lying in the street. There is no man standing on the street corner with a gun in his hand. It is not the kind of thing that people are used to. This presents a real challenge.

These issues and the opportunities they represent are proving to be very attractive to just about every country that has an information operations capability. For the nation state the potential of information warfare is something that's attractive, but it's also extremely threatening, because information warfare is not about nations; it's about the power that is given to individuals.

Information warfare is, I believe, fundamentally changing a dynamic that has existed for a very long time that has helped sustain stability between states, and that is that the government decides the pace of change, by and large, and is an instrument for a lot of the change.

When a new weapons system is developed, it takes quite a long time for that weapons system to go from the country that generated it to a country that does not have the capability to produce it. You are looking at a 20-year cycle. Today the latest computer is developed by Compaq, softwared by Microsoft, and is available at CompUSA, a computer store with outlets throughout the United States. Maybe, just maybe, the government might buy it within the next two or three years, but it's unlikely. Whereas, I can go to the computer store with my checkbook in hand and buy it. In an information war, that is my weapon.

I have the power, the capability, sitting in my home with my computer and my modem — if I only understood how to do it — to wage war. That is a very different environment than anything that we have experienced in the past.

It is particularly interesting, I think, that what we are seeing as the information revolution unfolds — and we're only at the very, very, very beginning of it — is the new range of alliances that is emerging. I recently talked to a friend who had put together an on-line conference of mountain men. These are people who live in the mountains all over the world — whether it be the Alps or the Urals or the Rockies or wherever — and they had a two-day on-line conference. These people who had never communicated before learned that they had a lot in common. They all hated the people in the valley. They all hated government, and they all cared passionately about the environment.

That's an example of a new community whose members have more in common with each other than they do, perhaps, with the other citizens of the nations in which they actually live. Now those groups — whether they are the 52 terrorist organizations who currently have web sites, environmental organizations, or people who simply feel disenfranchised — all have an opportunity to talk to each other, to share knowledge, and to express their frustrations. It's striking how there is a unity — or an ability to unite — among these groups that never existed before.

While we do not have the ability to eliminate the likelihood of war, we have the offensive ability to wage war by other means and certainly change the way we escalate to traditional conflict. And that presents some real challenges. First of all, government has to understand what war means. We are still locked into a Cold War environment. If you ask the Air Force or the Navy or the others who are developing these capabilities, "When are you allowed to use what you have?" they say, "Well, we asked the Justice Department that question a couple of years ago, and they haven't answered yet."

That is a big issue. These weapons are designed to be used exactly before we go to war to prevent us from going to war in the traditional sense. And yet they are very aggressive and very powerful. That is going to be a very big challenge for government. It already is. How does government remain relevant when everything around it is changing at such a pace?

We also, in a defensive way, have to deal with a different type of threat. Traditionally the military has seen itself as soldiers who go to the front line, fight, get wounded, die, or come back; they either succeed or they fail. But in the new environment, all of us are actually on the front line. The issue is how we defend and protect ourselves as well as how we are protected by government or by the private sector. We are part of the process. This represents a very different environment.

The Y2K (year 2000) computer problem is a very good illustration of this. It's actually a social issue, just as information warfare is a social issue. Information warfare is about turning off the water supply, cutting the power, making the wastewater treatment plants fail, stopping the ATM (bank automatic teller machine) systems, taking away the fabric of life.

Dealing with Y2K is going to demonstrate the scope of the interdependence of critical infrastructures. We don't yet — any of us — fully understand how interconnected everything we do is. If one piece of the puzzle falls out, the rest of the puzzle fragments as well. It's not just a national issue, it's an international issue.

So as we move forward addressing the challenges of information warfare, we have to address at the same time the challenges of government. What does that mean in this new environment? We have to address the challenge of the critical infrastructure. How do we defend that adequately?

A vital element is the private sector because it's the private sector that is the engine now driving the change unfolding around us. The government has to demonstrate its relevance and to take some form of leadership here, which I believe is noticeably absent.

The private sector can articulate many of these things to defend itself and, thus, to defend each one of us. If we fail to recognize that, I think we will experience some very serious trouble, beginning with Y2K. We will become victims of the new aggressors out there, who will have power that we have never really begun to understand, and when we understand it, it will be too late.

What I would argue is to try to educate people about these issues and to encourage not only public awareness but more action by those who have the ability to spread the word and, thus, create defenses against what is going to be an extremely aggressive environment in the next century.

FACT SHEET: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES

(Presidential Decision Directive 63)

The following fact sheet on Presidential Decision Directive 63 was released by the White House on May 22, 1998.

This Presidential Directive builds on the recommendations of the President's Commission on Critical Infrastructure Protection. In October 1997 the Commission issued its report, calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services.

Presidential Decision Directive 63 is the culmination of an intense, interagency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. The President's policy:

— Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000, by:

  a) Immediately establishing a national center to warn of and respond to attacks.
  b) Building the capability to protect critical infrastructures from intentional acts by 2003.

— Addresses the cyber and physical infrastructure vulnerabilities of the federal government by requiring each department and agency to work to reduce its exposure to new threats;

— Requires the federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;

— Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships;

— Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nation's economic power, not to stifle it.

— Seeks full participation and input from the Congress.

PDD-63 sets up a new structure to deal with this important challenge:

— a National Coordinator whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the United States may not come labeled in neat jurisdictional boxes;

— The National Infrastructure Protection Center at the Federal Bureau of Investigation, which will fuse representatives from the FBI, the Department of Defense, the U.S. Secret Service, the Departments of Energy and Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector. The Center will also provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts;

— An Information Sharing and Analysis Center is encouraged to be set up by the private sector, in cooperation with the federal government;

— A National Infrastructure Assurance Council drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan;

— The Critical Infrastructure Assurance Office will provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan. The office will also help coordinate a national education and awareness program, and legislative and public affairs.

For more detailed information on this Presidential Decision Directive, contact the Critical Infrastructure Assurance Office at (703) 696-9395 for copies of the White Paper on Critical Infrastructure Protection.

Cyberthreat: Protecting U.S. Information Networks: ARTICLE ALERT

Bennett, Robert, et al. THE Y2K CRISIS: A GLOBAL TICKING TIME BOMB? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 147-166)

Management consultants, financial planners, and experts in year 2000 conversion issues warn, in five essays, that the Y2K computer problem deserves to be taken seriously — and soon, before it is too late. Senator Bennett, who chairs a Senate Special Committee on the Y2K problem, says the "biggest challenge" is "to get people thinking... across the individual lines of our own organizations, indeed across the individual lines of our own country's borders." And "we must...recognize that this is not an IT (information technology) problem" but rather "a management challenge" that must be addressed immediately at the highest levels, he says.

Bowers, Stephen R. INFORMATION WARFARE: THE COMPUTER REVOLUTION IS ALTERING HOW FUTURE WARS WILL BE CONDUCTED (Armed Forces Journal International, August 1998, pp. 38-39)

Contending that access to information today is just as crucial as possession of petroleum and ammunition, Bowers discusses the threat posed by "almost invisible computer assailants" to a nation's power grids, transportation networks, financial systems, and telephone exchanges. He says recent U.S. military exercises have involved actions that elevate IW (information warfare) from a tactical to a strategic level. IW involves a new kind of battlefield but with the potential for equally as many casualties, he says.

Gompert, David C. NATIONAL SECURITY IN THE INFORMATION AGE (Naval War College Review, vol. 51, no. 4, sequence 364, Autumn 1998, pp. 22-41)

Gompert, director of the National Defense Research Institute at RAND, argues that the changes brought about by the information revolution, though not without drawbacks, have greatly benefited the United States. The information revolution has extended economic and political freedom, Gompert states, expanding the world's "democratic core." It has brought about significant changes in the conduct of warfare, giving the United States, with its lead in information technology, a great advantage: "Roughly stated, information technology can help those who master it to win large wars at long distances with small forces," says Gompert. He cites a concern that rogue states "are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information warfare (IW) attacks against the United States and its partners."

Henry, Ryan; Peartree, C. Edward. MILITARY THEORY AND INFORMATION WARFARE (Parameters, vol. 28, no. 3, Autumn 1998, pp. 121-135)

The authors examine the limited influence that technologies have had on warfare and cite as an example the airplane, which, though adding an unprecedented technological breakthrough to the battle space, repeatedly has been shown to be insufficient in and of itself to transform war. Old weapons do not necessarily go out of style — "new tools are just added to the box," the authors say. Underscoring the importance of grasping "the functional significance of technological innovations," they contend "it is equally important that risks and vulnerabilities — the stuff of strategy — remain foremost in assessing their political and military implications. The most durable military theory focuses less on the latest technology and more on the infinite complexity of the user."

Selden, Zachary. MICROCHIPS AND THE MILLENNIUM: THE NATIONAL SECURITY IMPLICATIONS OF THE YEAR 2000 PROBLEM (National Security Studies Quarterly, vol. 4, issue 3, Summer 1998, pp. 71-77)

Selden predicts that most computer software associated with the year 2000 problem will be fixed or discarded and that most of the problematic embedded computer chips will be replaced by January 1, 2000. What remains could cause unpredictable failures or sow confusion sufficient to allow states or terrorists to conduct covert disruptions or intrusions, he says. International actors may seek "to take advantage of a distracted United States" at the turn of the millennium, the author warns, and some current regional flash points might erupt "into a spiral of conflict because of failed systems." From a national security perspective the problem "is the perception that Y2K presents a window of vulnerability," the author says.

The annotations above are part of a more comprehensive Article Alert offered on the home page of the U.S. Information Service: "http://www.usia.gov/admin/001/wwwhapub.html".

Cyberthreat: Protecting U.S. Information Networks: BIBLIOGRAPHY

Adams, James. THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE. New York: Simon & Schuster, 1998. 366p.

Arquilla, John; Ronfeldt, David F. (Editors). IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE. Santa Monica, CA: Rand, 1997. 501p.

Barnett, Roger W. INFORMATION OPERATIONS, DETERRENCE, AND THE USE OF FORCE (Naval War College Review, vol. 51, no. 2, Spring 1998, pp. 7-19)

Browne, J.P.R.; Thurbon, M.T. ELECTRONIC WARFARE, Vol. 4 of Brassey's Air Power: Aircraft Weapons Systems and Technology Series. Washington: Brassey's, 1998. 341p.

Cillufo, Frank J.; Tomarchio, Thomas. RESPONDING TO NEW TERRORIST THREATS (Orbis, vol. 42, no. 3, Summer 1998, pp. 439-452)

Clinton, William J. COMMENCEMENT ADDRESS AT THE UNITED STATES NAVAL ACADEMY IN ANNAPOLIS, MARYLAND (Weekly Compilation of Presidential Documents, vol. 34, no. 21, May 22, 1998, pp. 944-948)

Copley, Gregory R. RE-DEFINING PSYCHOLOGICAL STRATEGY IN THE AGE OF INFORMATION WARFARE (Defense & Foreign Affairs Strategic Policy, vol. 26, no. 6, June 1998, pp. 5-8)

Gunther, Christopher. YOU CALL THIS A REVOLUTION? (Foreign Service Journal, vol. 75, no. 9, September 1998, pp. 18-23)

Henry, Ryan; Peartree, C. Edward (Editors). INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Significant Issues Series, vol. 20, no. 1). Washington: Center for Strategic & International Studies, 1998. 216p.

Libicki, Martin C. INFORMATION WAR, INFORMATION PEACE (Journal of International Affairs, vol. 51, no. 2, Spring 1998, pp. 411-428)

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR. Santa Monica, CA: Rand, 1996. 90p.

Petersen, John L.; Wheatley, Margaret; Kellner-Rogers, Myron. THE YEAR 2000: SOCIAL CHAOS OR SOCIAL TRANSFORMATION? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 129-146)

Pfaltzgraff, Robert L.; Schultz, Richard H. (Editors). WAR IN THE INFORMATION AGE: NEW CHALLENGE FOR U.S. SECURITY POLICY. Washington: Brassey's, 1997. 320p.

Rathmell, Andrew. INFORMATION WARFARE: USA TACKLES CYBERTHREAT (Jane's Intelligence Review Pointer, vol. 5, no. 9, September 1, 1998, p. 14)

Ryan, Stephen M. SHOULD U.S. PLEDGE NOT TO MAKE FIRST CYBERSTRIKE? (Government Computer News, vol. 17, no. 24, August 3, 1998, p. 32)

Sanz, Timothy L. INFORMATION-AGE WARFARE: A WORKING BIBLIOGRAPHY (Military Review, vol. 78, no. 2, March-April 1998, pp. 83-90)

U.S. Senate, Select Committee on Intelligence. CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES. Washington: Government Printing Office, 1998. 177p.

Verton, Daniel. DOD PREPS OFFICE FOR CYBERDEFENSE (Federal Computer Week, vol. 12, no. 23, July 13, 1998, pp. 1-2)

Cyberthreat: Protecting U.S. Information Networks: KEY INTERNET SITES

Please note that USIS assumes no responsibility for the content and availability of the resources listed below; such responsibility resides solely with the providers.

Air Force Information Warfare Center
http://www.afiwc.aia.af.mil/

Center for High Assurance Computer Systems of the Naval Research Laboratory
http://www.itd.nrl.navy.mil/ITD/5540/main.html

Computer Security Technology Center, Lawrence Livermore National Laboratory, U.S. Department of Energy
http://ciac.llnl.gov/cstc/

Critical Infrastructure Assurance Office
http://www.ciao.gov/

Cyberspace Policy Institute at George Washington University
http://www.seas.gwu.edu/seas/institutes/cpi/

Defense Information Infrastructure
http://spider.osfl.disa.mil/dii/

Defense Policy on the Year 2000 Computer Conversion Issue
http://www.defenselink.mil/issues/y2k.html

Glossary of Information Warfare Terms
http://www.psycom.net/iwar.2.html

IBM Corporation: Secure Way
http://www.ibm.com/Security/

Information Systems Security Association
http://www.issa-intl.org/

Information Warfare Academic Group, Naval Postgraduate School
http://web.nps.navy.mil/~iwag/

Information Warfare and Information Security on the Web
http://www.fas.org/irp/wwwinfo.html

Information Warfare: Glossary
http://www.informatik.umu.se/%7Erwhit/IWGlossary.html

Information Warfare Research Center
http://www.terrorism.com/infowar/documents.html

InfoWar.Com
http://www.infowar.com/main.html

Infrastructure Defense, Inc.
http://206.132.10.154/idmarketsite/

Microsoft Corporation (Key Initiatives)
http://www.microsoft.com/

National Colloquium for Information Systems Security
http://www.infosec.jmu.edu/ncisse/

National Infrastructure Protection Center of the Federal Bureau of Investigation
http://www.fbi.gov/nipc/home.htm

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/

National Security Agency
http://www.nsa.gov:8080/

President's Council on Year 2000 Conversion
http://www.Y2K.gov/java/index.htm

School of Information Warfare and Strategy, National Defense University
http://www.ndu.edu/inss/act/iwscvr.html

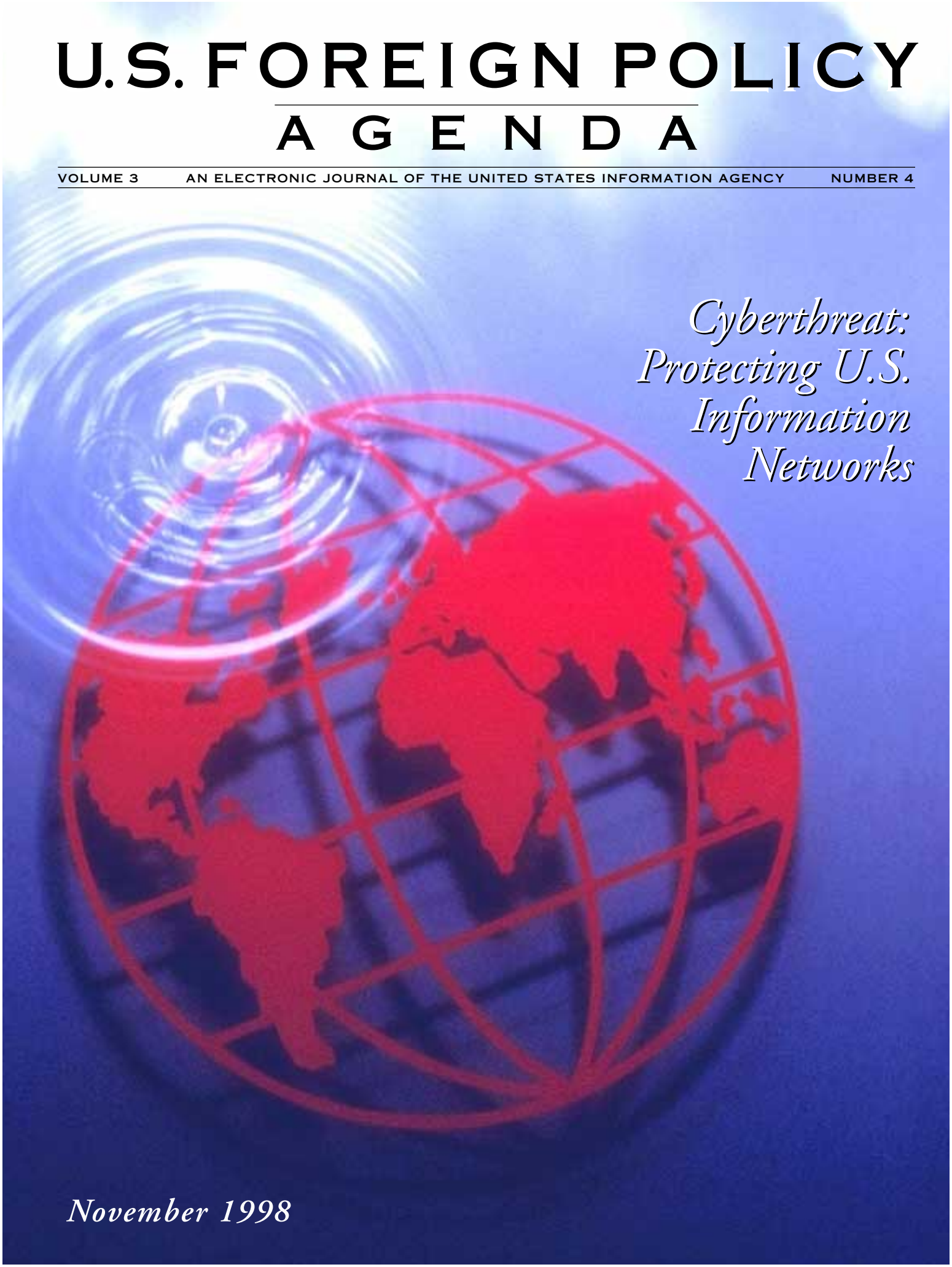
Technology News: Governments Beat Terrorists To Net Weapons
http://www.techweb.com:80/wire/story/TWB19980922S0018

U.S. Senate, Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information
http://www.senate.gov/~judiciary/terrtest.htm

Year 2000 Conversion: U.S. Information Agency
http://www.usia.gov/topical/global/y2k/

U.S. FOREIGN POLICY AGENDA

VOLUME 3 AN ELECTRONIC JOURNAL OF THE UNITED STATES INFORMATION AGENCY NUMBER 4



Cyberthreat: Protecting U.S. Information Networks

November 1998