SECURITY IN THE INFORMATION AGE

NEW CHALLENGES, NEW STRATEGIES

JOINT ECONOMIC COMMITTEE
UNITED STATES CONGRESS

MAY 2002

Security in the Information Age: New Challenges, New Strategies

Joint Economic Committee
United States Congress

May 2002

Joint Economic Committee
G01 Dirksen Senate Office Building
Washington, D.C. 20510
Phone: 202-224-5157
Fax: 202-224-0240
Internet Address: http://www.house.gov/jec

Foreword

Over the years, the Joint Economic Committee has investigated a wide range of threats to the United States and its economy. The committee has consistently identified emerging issues including radio frequency weapons, bioterrorism, information warfare, espionage, technology transfers, transnational crime, and weapons proliferation. We continued that course in June 2001 with a hearing entitled, "Wired World: Cyber Security and the U.S. Economy." Following this hearing, it became clear that we needed to better understand an increasingly complicated set of diffuse security threats. Senator Bennett volunteered to identify individuals whose perspectives about critical infrastructure protection would be of value to the Congress and compile a study.

Computer networks connect and control everything from pipelines to stock exchanges. At a speech given on March 23, 2001, to the Partnership for Critical Infrastructure of the U.S. Chamber of Commerce, Condoleeza Rice, United States National Security Advisor said, "Today, the cyber economy is the economy. . . . Corrupt those networks and you disrupt this nation."

The September 11 attacks on the World Trade Center and the Pentagon make it clear that we must be better aware of our vulnerabilities and develop viable strategies to detect, deter, and counter both physical and cyber-based threats to our people and our infrastructures.

This compendium represents a range of perspectives on infrastructure protection, from definitions and strategies to business challenges and policy actions. I thank Senator Bennett for his efforts and the authors for sharing their expertise.

Jim Saxton
Chairman

Table of Contents

Security in the Information Age: We're Not in Kansas Anymore

By Senator Robert F. Bennett

It is very important to concentrate on hitting the U.S. economy through all possible means . . . look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck . . .

—Osama Bin Laden, December 27, 2001

Be Prepared.

—Boy Scout Motto

Toto, I've a feeling we're not in Kansas anymore.

—Dorothy, *The Wizard of Oz*

The attacks of September 11 hit Americans like a sudden midwestern tornado. For the first time since Pearl Harbor we suddenly started asking ourselves, "How vulnerable are we? And where?" The anthrax attacks in October helped give us the answers: "very"and "everywhere."

The infrastructures deemed critical are "so vital that the incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[1] Where security once meant digging a moat around the castle, now it must involve whole industries and systems. Telecommunications, energy, banking and finance, transportation, water, emergency services, and essential government service are now connected to each other in one way or another in this "wired" age.

To ensure that America continues to function in this new world of interdependent vulnerabilities, government must work closely with the private sector in a series of new, cooperative ways.

Ensuring that essential services and industries survive a crisis has always been a part of our national security strategy. What is new is (1) computer networks have created extremely complex linkages and interdependencies that have never existed before, and (2) the majority of critical infrastructures are outside federal control. Consequently, identifying what is critical is becoming both more difficult and more vital. The Information Age, in bringing us an exciting new era of technology, has also given us a new set of security problems.

On June 21, 2001, Lawrence K. Gershwin of the National Intelligence Council told the Joint Economic Committee that the "information technology revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid 18th-century . . . no country in the world rivals the United States in its reliance, dependence, and dominance of information systems. The great advantage we derive also presents us with unique vulnerabilities."[2]

Computer networks create new avenues for those with malicious intent. While still vulnerable to actual destruction by physical attacks, such as bombs or arson, these networks are targets of threats of mass disruption. Our economy can be crippled by strategic information warfare in the form of computer intrusions, scrambling software programs, undetected insiders within computer firewalls, or cyberterrorists around in the world.

Severity of computer attacks can vary from mere annoyances that disrupt business for a few hours to attacks designed to shut down or cripple entire systems. In a hearing before the Senate Subcommittee on Technology, Terrorism, and Government Information, Arizona Attorney General Janet Napolitano outlined a scenario in which a hacker had infiltrated the computer system of an Arizona dam, and threatened to open the floodgates. Fortunately, the hacker was a computer crimes specialist being paid to test the computer system.[3] If the attack had been malicious, the results would have included flood damage, severely diminished water supply, and major disruptions to power generation. The computer hack could have caused the same damage as a strategically placed bomb.

The integration of telecommunications and computer systems into energy, transportation, human services, telecommunications, finance, and civilian government sectors also includes the U.S. military. When the secretary of defense in the Pentagon places a telephone call, it is likely that a commercial telecommunications company will be providing the service. It has been estimated that over 95 percent of defense communications rely on the public phone system.[4]

In short, to ensure that America continues to function—that America's critical infrastructures are protected in this new world of interdependent vulnerabilities—government must work closely with the private sector in a series of new, cooperative ways.

A STRATEGY IS NEEDED

The acclaimed British strategic thinker B.H. Liddell-Hart approached strategy from two different perspectives. He differentiated between a "grand strategy" and

"military strategy." Liddell-Hart's "grand strategy" focused on a nation's ability to "coordinate and direct all resources of a nation" toward the attainment of a political objective. "Military strategy" was more narrow, related to the execution of a battle plan or the projection of military force.[5]

In our current circumstance, a broad perspective of "grand strategy" is needed, with no artificial distinctions between "homeland security" and "critical infrastructure." Because our vulnerabilities are complex and the threats are varied and unpredictable, it is impossible to protect everything from every threat.

Accordingly, we must develop a "grand strategy" by:

- Identifying what is critical and vulnerable.
- Increasing two-way information sharing between the public and private sectors.
- Improving analysis and warning capabilities.

IDENTIFYING WHAT IS CRITICAL AND VULNERABLE

In 1998, Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection described critical infrastructure as "those physical and cyber-based information systems essential to the minimum operations of the economy and government." PDD 63 called for an initial vulnerability assessment within 180 days of issuance, followed by periodic updates for each sector of the economy and each sector of the government that might be a target of infrastructure attack. These assessments were also to "include the determination of the minimum essential infrastructure (MEI) in each sector." The purpose of defining the MEI was to assess vulnerabilities, determine a remediation strategy, and better focus analysis and warning to ensure that the core components of the MEI would be unaffected by attempted attacks. However, PDD 63 did not establish a criteria for what was critical or create a process to identify critical assets to accomplish this goal.

In March 2001, the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency reported on the progress of these assessment activities. They found:

- Most agencies had not identified their mission-essential infrastructure assets.
- Almost none of the agencies had completed their vulnerability assessments of their MEI assets or developed remediation plans.[6]

The General Accounting Office (GAO) confirmed this assessment. In September 2001, the GAO released a comprehensive report that outlined what progress had been made since the issuance of PDD 63. The report attested that while efforts to establish partnerships and raise awareness have been progressing, substantive, comprehensive analysis has not. Without either a criteria or a process to identify critical infrastructure, assessing vulnerabilities and identifying a minimum essential infrastructure has progressed slowly. Development of related remedial plans has been moving slowly as well.[7]

The following chart highlights the status of assessments in various sectors:[8]

Infrastructure Sector	Vulnerability Assessment	Remedial Plan
Banking and finance	Some assessments	No remedial plans
Electric power, oil, and gas	Some assessments	No remedial plans
Emergency fire services	No assessments	No remedial plans
Emergency law enforcement	No assessments	No remedial plans
Information and communications	No assessments	No remedial plans
Public health services	No assessments	No remedial plans
Transportation	No assessments	No remedial plans
Water supply	Some assessments	No remedial plans

Government and industry cannot afford to protect everything to the same degree. As a result, chief executive officers and national and homeland security planners must prioritize. They must decide what core missions and supporting services are most critical. These respective efforts will likely result in competing concerns. Nevertheless, once critical needs are identified, competing priorities can be assessed and factored into contingency planning efforts.

Since the government does not own or operate the bulk of critical infrastructures, discerning their relative importance may be difficult. Ultimately there must be a sector-by-sector approach with the participation and cooperation of both government and industry.

INCREASING INFORMATION SHARING

A 1994 Joint Security Commission reported that "if instead of attacking our military systems and databases an enemy attacked our unprotected civilian infrastructure, the economic and other results would be disastrous."[9] The events of September 11 demonstrated the truth of this statement.

When the World Trade Center towers collapsed, so did the telephone system and the switches that reportedly handled three million data circuits. Electronic

transfers of billions of dollars ceased. Amid the rubble, disaster plans were put into effect, back-up systems turned on, and banks and businesses struggled to recover. Given the shock and the magnititude of such an attack, there are plenty of examples of things that were done right, before, during, and after the attack, particularly in the private sector. Central to this effort was information sharing and assistance across sectors and government to recover from the crises as quickly as possible.

The need to share information *before* a crisis is also important. The President's Commission on Critical Infrastructure Protection under the Clinton administration identified information sharing as one of the most pressing needs in protecting critical infrastructure. The report stated,

> The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns must give way to a concept of shared threats. Shared threats demand a shared response, built from increased partnerships between government and the owners and operators of our infrastructures.[10]

If both the private sector and the federal government are targets, it makes sense for two targets to share information with each other.

The private sector is on the front line, yet has no access to government information about possible threats, much of which is often classified. On the other hand, the federal government, which has unique information and analytical capabilities, lacks specific information about attacks—particularly computer attacks—occurring outside the government but still within the United States. Both parties have a blind spot and only see parts of the problem. In addition, the potential range of attacks, particularly computer-based, makes them very difficult to understand or analyze. Government and industry would benefit from cooperating in response to threats, vulnerabilities, and actual attacks by sharing information and analysis.

Although information sharing between the government and private sector may be desirable, the private sector has identified factors that impede such information sharing. Foremost is a fear that sensitive information would not be protected from disclosure, deliberate or inadvertent. Deliberate disclosure would come if sensitive data voluntarily shared with the government were released under the Freedom of Information Act (FOIA). It is important to note that the ability for persons to obtain information under FOIA is not limited to American citizens

interested in seeing what the federal government is doing. It also includes foreign citizens, partnerships, corporations, associations, and even foreign governments. Critical infrastructure information from the private sector could include information about threats against an industry's own assets. This information is not normally in the public domain, and should it be released to the public, it could be used as a road map for future terrorist attacks or for undermining a company's competitiveness.

An inadvertent release of critical infrastructure information to the general public is also a concern. Currently there are no uniform procedures for handling this type of information across government agencies. The dangers that exist with an accidental release of confidential business information, such as trade secrets or proprietary information, are the same for the inadvertent risk of sensitive information about critical infrastructure: "damaged reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms."[11] In the current environment, accidental release could also increase the vulnerability of an infrastructure to attack.

Congress has acted at least 60 different times to protect certain information from public disclosure to account for needs in specific circumstances. For example, taxpayer information, South Pacific tuna fishing license holder information, crop insurance proposals, classified national security information, and smokeless tobacco ingredients are not disclosed to the public. Such information can be withheld under FOIA. However, a power operator who wants to share information about attacks against their computerized systems cannot share this information with the government with the same certainty.

In response to the growth of cyberattacks on networked systems, PDD 63 encouraged the development of Information Sharing and Analysis Centers (ISACs). These centers have been established in banking, telecommunications, electric power, emergency law enforcement, and information technology. ISACs are organizations whose members can report and exchange information relating to threats, vulnerabilities, attack solutions, countermeasures, best practices, and other protective measures. They play a key role in helping to understand threats to infrastructures.

While ISACs have the potential to play an important role in support of economic and national security, they have some limitations. First, not all critical industries are members of ISACs. In additional, ISACs are evolving industry by industry and are being developed to meet the specific security needs of each sector. Sole dependence on an industry-specific focus fails to give government or industry crosscutting information that would be helpful in establishing broad patterns or threats that go beyond a single sector.

IMPROVING ANALYSIS AND WARNING

Information without analysis has little use. For example, various industries in Washington, Michigan, Kansas, and Massachusetts may report seemingly unrelated computer or physical attacks. A pattern may only be discernable as attacks if that information were analyzed by one entity. Accordingly, there should be an entity tasked with coordinating the analysis of critical infrastructure threats and the development of a warning system both for cyber-based and physical threats. Any entity tasked with this mission will need to have clear authority, resources, and significant interagency support to be successful. While this may sound easy, it is an extremely complex challenge that could require years to achieve.

Learning to identify potential patterns of attack, detecting surveillance of computer systems, or discerning the intent of seemingly widespread or random computer viruses or worms will require a new discipline. Tomorrow's terrorists may employ a wider range and combination of destructive tools. "Viruses and worms are likely to become more controllable, precise, and predictable, making them more suitable for weaponization. . . . The tools for distributed hacking or denial of service—the coordinated use of multiple, compromised computers or of independent and mobile software agents—will mature as network connectivity and bandwidth increase."[12]

In concert with efforts to improve analytical capabilities, there is a need for a warning process for critical infrastructures. It is important to recognize that the process should include both the sending *and* the receipt of information. Since September 11, more attention has been paid to warnings. The Office of Homeland Security has unveiled a warning system for the country. However, a common system of warning that is applicable to all of the infrastructures would be most useful. Such a system would include not only a clearly defined scale or levels, but a corresponding set of proposed actions. The establishment of such a system will require a significant interagency effort to coordinate responsibilities.

In addition to developing a clearly defined dissemination capability, government and industry must develop a way for determining whether information has been received and action taken. Currently, the media is the default measure to determine if warnings are useful. When we read that people took action and the problem was avoided, there is usually a follow-up story that claims that the threat was hyped and the warning was too strong. (We saw this with regard to Y2K.) If people fail to take action, we will likely read the warning wasn't strong enough. It is difficult to imagine a scenario which media reports alone will provide information specific enough to be useful.

While organizations with some analytical and warning capabilities exist in the Departments of Justice and Commerce, universities, and the private sector, and now Homeland Security, our capacity must be far more robust. Our ability to analyze information and develop an effective warning process directly effects the ability to defend the nation's infrastructures.

CONCLUSION

America is facing a steep learning curve as it begins to assess its new technological vulnerabilities and security threats. We must begin developing a strategy that includes the private sector and the government, utilizing the strengths of each. A comprehensive strategic approach to infrastructure protection must include identifying what is critical and vulnerable, increasing information sharing, and improving analysis and warning.

It is imperative to think "horizontally," to be mindful of the connections between physical buildings and networks in cyberspace that create complex interdependencies in which the weakest links become targets. These interdependencies require us to think differently about security. I invite you to explore these issues further by reading this study.

An Overview of Infrastructure Assurance

Kenneth Juster and John Tritak provide a conceptual overview of infrastructure assurance. They outline a number of challenges related to who protects infrastructures and what the role of the federal government is in ensuring essential government services and orderly operation of the national economy.

Cyber Security Policy

Advocating the need for a true national debate on infrastructure assurance, Mark Montgomery outlines a need to rethink national security strategy—and, by extension, economic security and our nation's security. He defines a solid approach to critical infrastructure protection and information assurance centered on three "prongs": policy, technology, and people. He calls for closer federal private partnerships: "Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses."

National Information Power

William Gravell introduces the idea of a comprehensive "national information strategy" designed to support a broad range of policy goals. Gravell promotes a

balanced approach to this new strategic concept so it may defend a defined set of information equities, deliberately culled from the vast body of information that surrounds our daily lives.

Cyber Early Warning

Strategic early warning capabilities enabled the U.S. to detect and deter potential nuclear attacks. David Keyes compares the components of historical warning models to early warning for cyberattacks demonstrate the complexity of the challenge. The author also discusses the need to review burden sharing for the development of warning capabilities and identifies a series of private sector issues requiring more thoughtful consideration.

Transitions between Law Enforcement and National Defense

In response to criminal activity, law enforcement and national security personnel have struggled to remain effective in an increasingly complex technological world. Authors Scott Charney and Angeline Chien discuss the difficult transitions between law enforcement and national defense and the integration of these respective efforts. Charney addresses the security dilemma, the public safety/ national security conundrum and the evolving role of private markets. In a complementary piece, Chen outlines the potential synergies between defense and law enforcement, and the evolution of existing capabilities and future requirements.

The Defense Production Act and CIP

Close to five years after the President's Commission on Critical Infrastructure issued its report, the nation still lacks an integrated legal, policy, and management philosophy to support critical infrastructure protection efforts. Lee Zeichner explores the Defense Production Act (DPA) as one of the most significant congressional authorities for supporting infrastructure protection efforts and managing infrastructure disruptions of national significance.

Definitions of National Security

Jack Oslund examines the challenges related to defining national security and national interests in the context of the changing geopolitical environment. He places a particular emphasis on the challenges of diffuse and asymmetrical threats and the rapid increase in global connectivity and technological interdependence.

Counterintelligence and CIP

Identifying the inseparability of critical infrastructure protection and counter-intelligence, John MacGaffin points to the need for collaborative federal-private efforts to address a wide range of policy challenges. MacGaffin details a list of issues which must be resolved and highlights some promising counterintelligence initiatives already underway.

Risk Management

Nancy Wong discusses the risk management process involved in assuring delivery of critical infrastructure services. She outlines a range of business approaches to prevention or deterrence, mitigation, and crisis management and recovery. While each institution has an economic and public interest to assure its own service, concerted attention and action is required to assure that disruptions to networks supporting one part of the infrastructure system do not cascade.

Michael Rasmussen examines critical infrastructure from a business perspective, particularly assuring stakeholder value in a digital age. He examines an approach beginning with (1) board members, (2) executives, (3) managers, (4) employees, and (5) business partners. While an effective information protection program is unique in every organization, Rasmussen discusses seven common steps which can be taken to implement an effective program.

Notes:

1. Executive Order 13010, Critical Infrastructure Protection, July 15, 1996.
2. Dr. Lawrence K. Gershwin, National Intelligence Office for Science and Technology, National Intelligence Council, Central Intelligence Agency, Hearing before the Joint Economic Committee, Congress of the United States, June 21, 2001.
3. Hearing of the Senate Subcommittee on Technology, Terrorism, and Government Information, held in Scotsdale, Arizona, as reported by the Associated Press, April 22, 2000.
4. Joint Security Commission, Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, available at http://www.dss.mil/seclib/jcs.htm#c8
5. B. H. Liddell-Hart, *Strategy* (New York: Signet Books, 1967), 321–322. See also, Gregory J. Rattray, *Strategic War in Cyberspace* (Cambridge, Massachusetts: MIT Press, 2001), 78–79.
6. Letter from the President's Council on Integrity and Efficiency/Executive Council on Integrity & Efficiency, to Mr. Richard A. Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, March 21, 2001.
7. Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822), September 11, 2000.
8. Ibid.

9. Joint Security Commission, Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, available at http://www.dss.mil/seclib/jcs.htm#c8
10. Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection, October, 1997.
11. Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822), September 11, 2000.
12. Dr. Lawrence K. Gershwin, National Intelligence Office for Science and Technology, National Intelligence Council, Central Intelligence Agency, Hearing before the Joint Economic Committee, Congress of the United States, June 21, 2001.

Critical Infrastructure Assurance: A Conceptual Overview

By Kenneth I. Juster and John S. Tritak

CRITICAL INFRASTRUCTURES: WHAT THEY ARE AND WHY THEY ARE IMPORTANT

Critical infrastructures comprise those industries, institutions, and distribution networks and systems that provide a continual flow of the goods and services essential to the nation's defense and economic security and the health, welfare, and safety of its citizens.

These infrastructures are deemed "critical" because their incapacity or destruction could have a debilitating regional or national impact. These infrastructures relate to:

- Information and communications
- Electric power generation, transmission, and distribution
- Oil and gas storage and distribution
- Banking and finance
- Transportation
- Water supply
- Emergency assistance

Critical infrastructure assurance is concerned with the readiness, reliability, and continuity of infrastructure services so that they are less vulnerable to disruptions, any impairment is short duration and limited in scale, and services are readily restored when disruptions occur.

RECENT CONCERN OVER CRITICAL INFRASTRUCTURE ASSURANCE

Assuring delivery of critical infrastructure services is not a new requirement. Indeed, the need for owners and operators to manage the risks arising from service disruptions has existed for as long as there have been critical infrastructures. As more is learned and understood about the characteristics of evolving physical threats such as terrorism, owners and operators generally have practices to build on to enhance their assurance programs.

What is new are the challenges to assured service delivery arising from an increased dependence on information systems and networks to operate critical infrastructures. This dependence exposes the infrastructures to new vulnerabilities. Individuals and groups seeking to exploit these vulnerabilities range from the recreational hacker to the terrorist to the nation state intent on obtaining strategic advantage.

The cybertools needed to cause significant disruption to infrastructure operations are readily available. One does not have to be a "cyber-terrorist" or an "information warrior" to obtain and use these new weapons of mass *disruption*. From the perspective of individual enterprises, the consequences of an attack can be the same, regardless of who the attacker is.

Because there are no boundaries or borders in cyberspace, and because the vast majority of the nation's infrastructures are privately owned and operated, government action alone cannot secure them. Only an unprecedented partnership between private industry and government will work.

To complicate matters further, each of the critical infrastructure sectors is becoming increasingly interdependent and interconnected. Disruptions in one sector are increasingly likely to affect adversely the operations of others. For example, loss of telecommunications services can impede financial service transactions and delivery of electric power. Similarly, there can be no e-commerce without "e"-electricity.

Moreover, our society, economy, and government are increasingly being linked together into an ever-expanding *national* digital nervous system. Disruptions to that system, however and wherever they arise, can cascade well beyond the vicinity of the initial occurrence, causing regional and, potentially, national disturbances.

Prior to the information age, critical infrastructure assurance was essentially a state and local concern. With the introduction of information technologies, however, it has become a national concern, with significant implications for the defense and economic security of the United States.

THE CHALLENGE: WHO PROTECTS CRITICAL INFRASTRUCTURE?

Threats to critical infrastructure fall into two general categories: (1) physical attacks against the "real property" components of the infrastructures, and (2) cyberattacks against the information or communications components that control these infrastructures.

Until recently, federal policy on the protection of national critical infrastructures against physical attacks has been largely implicit and indirect. At the enterprise level, infrastructure owners and operators have always had responsibility for protecting their physical assets against unauthorized intruders. Yet these measures, however effective they might otherwise be, were generally not designed to cope with significant military or terrorist threats. Nor did they have to be. The Defense Department, Justice Department, and other federal agencies have contributed significantly to the physical protection of the nation's critical infrastructures through the defense of national airspace against enemy bombers, and the defense of national borders against invading armies and infiltrating terrorists.

Securing the nation's critical infrastructures against cyberattacks presents a very different problem. Although owners and operators have primary responsibility for protecting their information assets, current efforts are uneven and spotty. In the aggregate, these efforts may not provide a level of security capable of safeguarding against systemic failures on a regional or national level. Nor can federal efforts entirely compensate for this security deficit. The federal government cannot post soldiers or police officers at the perimeters of electric power plants or telecommunications facilities to keep out digital attackers.

Because there are no boundaries or borders in cyberspace, and because the vast majority of the nation's infrastructures are privately owned and operated, government action alone cannot secure them. Only an unprecedented partnership between private industry and government will work.

WHAT NEEDS TO BE DONE?

The federal government has two interests in critical infrastructure assurance—assuring essential government functions and services and ensuring an orderly functioning of the national economy. Each of these tasks requires a close working relationship with private industry for its advancement. In addition, there needs to be a national planning process to coordinate the respective activities of government and industry in these endeavors.

Essential Government Functions and Services

One interest is the assured performance of essential functions and services by the federal government in accordance with its Constitutional obligations to "provide for the common defense," "promote the general welfare," and "insure domestic tranquility." Such functions and services are vital to advancing our national security, foreign affairs, economic prosperity and security, social health and welfare, and public law and order. Examples include: the mobilization and

projection of U.S. forces overseas, the ability to maintain critical government communications during crises involving national security or a national emergency, the provision of timely warnings of potential weather disturbances, and even something as basic yet important to a significant segment of the population as the delivery of social security checks.

Increasingly, these services depend ultimately on privately owned and operated infrastructures. Thus, to advance this vital federal interest, the government must take a leading role and satisfy a number of requirements. Each federal department and agency must identify: (1) its essential functions and services and the critical assets responsible for their performance, (2) all associated dependencies on assets located in other departments and agencies that are necessary to performance or delivery, and (3) all associated dependencies on privately owned and operated critical infrastructures that also are essential to performance or delivery.

To illustrate, the Commerce Department is responsible for providing timely warnings of hurricanes through its Tropical Prediction Center (the "TPC") in Miami, Florida. Incapacity or destruction of this essential government service could result in considerable loss of life and property. Indeed, thousands of people died during the Galveston, Texas hurricane of 1900 because there was no advance warning of the hurricane's approach and, thus, no one evacuated the city. In 1992, Hurricane Andrew would have been even more devastating than it was had the TCP not been able to provide timely information about the storm, thereby enabling thousands to evacuate from those areas where the storm's predicted strength threatened to be greatest.

Although the TPC is a critical asset, it does not operate in isolation; it depends on a variety of other government agency assets, as well as assets owned and operated by private government contractors. These include satellite imaging and analysis centers and radio transmission facilities located in Maryland and Pennsylvania. Operational disruptions at any one of these facilities could impede the delivery of timely hurricane warnings just as effectively as operational disruptions at the TPC itself. Furthermore, the TPC depends on specific providers of critical infrastructure services to operate, including Florida Power & Light for electric power, and Bell South & MC 2000 for telecommunications. Disruptions to these services also could impede TCP operations that are necessary to deliver hurricane warnings.

Once such critical assets and associated dependencies are identified, federal departments and agencies must assess their vulnerability to physical or cyber-attack. If they are determined to be vulnerable, departments and agencies must develop and implement plans to manage the risks posed by potential attacks to the performance of essential functions and services. These plans should seek to deter attacks from happening in the first place, protect critical assets from damage or

destruction if attacks occur, mitigate the operational impact of attacks if protective measures fail, restore operations if attacks disrupt services, and reconstitute assets if damaged or destroyed during attacks. Where performance of essential government functions and services depends on privately owned and operated infrastructures, federal departments and agencies must work with the owners and operators of these specific infrastructure companies—on mutually agreed upon terms—to ensure adequate security measures are established and maintained.

Orderly Functioning National Economy

The second federal interest is to ensure a sufficient level of critical infrastructure services to maintain an orderly functioning national economy. The preferred approach to advancing this interest is to promote market rather than regulatory solutions, with the federal government playing three important supporting roles.

Promote National Awareness

The first role is to raise national awareness about the problem of critical infrastructure assurance. The primary focus of these efforts should be on the critical infrastructure industries. The target audience should be the corporate boards and chief executive officers who are responsible for setting company policy and allocating company resources. The basic message is that critical infrastructure assurance is the core business of the critical infrastructure institutions. Consequently, it is a matter for corporate governance and risk management. Senior management has always understood that they are responsible for securing corporate assets. Today, those corporate assets include information and information systems. Corporate boards will need to understand, if they do not already, that they are accountable, as part of their duty of care, to provide effective oversight of the development and implementation of appropriate infrastructure security policies and practices.

The challenge of a national awareness effort is to present a compelling business case for corporate action. Generally, government concerns about economic and national security do not provide such a case. Unlike physical threats, threats of "cyberterrorism" and "information warfare," while legitimate, are not readily executable in the market—they appear too remote and irrelevant to a company's bottom line.

Only when the threats to critical infrastructure are translated into business terms that corporate boards and senior management understand, such as operational survivability, shareholder value, customer relations, and public confidence, will companies respond more positively. Only when corporate leaders understand that in addition to physical means, the electronic tools capable of disrupting their

operations are readily available, and not the monopoly of terrorist groups or nation states, will they conclude that the risks to their companies are serious and immediate and, thus, require their prompt attention.

In addition to infrastructure owners and operators, awareness efforts also should target other influential stakeholders in the economy. The risk management community—including the audit and insurance professions—is particularly effective in raising matters of corporate governance and accountability with boards and senior management. In addition, the investment community is increasingly interested in how information security practices affect shareholder value—a concern of vital interest to corporate boards and management.

Facilitate Corporate Action

Once the private sector acknowledges the problem of critical infrastructure assurance as one that it must solve through corporate governance and risk management, a second role for the government is to facilitate corporate action.

The government should encourage information sharing within and among the infrastructure sectors and, as appropriate, between the sectors and government. The information shared could include system vulnerabilities, cyber-incidents, trend analyses, and best practices. The reason companies should be encouraged to share this kind of information is because by doing so they will obtain a more accurate and complete picture of their operational risks, as well as acquire the techniques and tools for managing those risks.

The government also should encourage and facilitate the infrastructure sectors to work together on developing contingency plans for coordinating their responses in the event of major service disruptions, whatever the precipitating cause. As the infrastructures become more interdependent, there is a growing risk that restoration efforts undertaken by one sector could adversely affect the operations or restoration efforts of another, potentially contributing to further service disruptions.

In addition, the government should work with industry in identifying potential legal and regulatory obstacles that may impede information sharing or might otherwise interfere with voluntary efforts by the business community to maximize information security efforts. For example, some in industry have argued that voluntary information sharing cannot proceed to a fully mature corporate activity until the reach and impact of laws governing antitrust and tort liability and the Freedom of Information Act are clarified.

Direct Federal Support

Finally, the government needs to acknowledge that there are limits to how far the private sector will go in securing its infrastructure in response to market forces and concerns for corporate governance. Where this occurs, the government must explore other options to prevent market failures from posing an unacceptable risk to the economic and national security of the United States. For example, the federal government needs to anticipate and prepare for instances where it or coordinated state and local government will have to become actively engaged in coordinating the restoration efforts of one or more infrastructure sectors where refraining from doing so could result in service disruptions spreading to other sectors or to other regions of the country.

The federal government also will need to identify areas of research and development that the market is unlikely to pursue. One such area is interdependency analysis and modeling. Little is currently known about how specific types of disruptions in one infrastructure sector affect the operations of the others. Improving our understanding in this area and developing predictive tools for assessing the potential impact of service outages on various sectors of the economy—and government—are essential to developing better means for early warning and response.

Development of a National Strategy

A common means of communicating overall critical infrastructure policy is essential. A national strategy developed jointly between government and industry is an effective means for arriving at a consensus about respective roles and responsibilities. A national strategy also helps to establish the basis with the Congress and the American public for proposing legislative and public policy reforms where such reforms are needed to advance national policy.
The development of a national strategy should not be viewed as an end in itself. It should be part of a dynamic process in which government and industry continue to modify and refine their efforts at critical infrastructure assurance, adjust to new circumstances, and update the strategy as appropriate.

Kenneth I. Juster was nominated by President Bush on March 15, 2001 to be the Under Secretary of Commerce for Export Administration. Prior to joining the Bush administration, Mr. Juster was a senior partner in the law firm of Arnold & Porter. He has broad experience in U.S. foreign policy, international trade and transactions, and dispute

resolution. His practice included counseling clients with regard to foreign investments, the application of U.S. economic sanctions and trade controls, and public policy issues.

John S. Tritak is Director of the Critical Infrastructure Assurance Office (CIAO). As Director, Mr. Tritak is responsible for supporting the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism in the development of an integrated National Infrastructure Assurance Plan to address threats to the nation's critical infrastructures, including communications and electronic systems, transportation, energy, banking and finance, health and medical services, water supply, and key government services. Before joining the CIAO, Mr. Tritak was an attorney with the law firm of Verner, Liipfert, Bernhard, McPherson, and Hand, Chartered. Mr. Tritak served as Deputy Director for Defense Relations and Security Assistance in the State Department's Bureau of Politico-Military Affair. Mr. Tritak also served as a State Department adviser to the U.S. delegation negotiating the Strategic Arms Reduction Treaty in Geneva, Switzerland.

Mr. Tritak received a B.S. in Political Science from the State University of New York at Brockport, an M.A. in War Studies from the University of London, Kings College, and earned his J.D. from the Georgetown University Law Center.

Cybersecurity Policy: Moving from Nouns to Verbs

By Mark Montgomery

For too long our cybersecurity efforts have focused on the "beep and squeak" issues, and have been attracted to the individual virus or hacker in the news, often to the neglect of the bigger picture, incorporating the economy and beyond. It is time to identify gaps and shortfalls in our current policies, programs, and procedures; begin to take significant steps forward; and pave the way for the future by laying down the outlines of a solid course of action that will remedy existing shortcomings.

We need a true national debate on infrastructure assurance and we need to rethink national security strategy—and by extension, economic security and our nation's security—accordingly.

This even more timely because the executive branch is currently drafting a new national plan to provide guidance and direction for cybersecurity. It is scheduled to be released by year's end. Likewise, an Executive Order (EO) on the same subject, entitled "Critical Infrastructure Protection in the Information Age," is near completion. And, in his first National Security Presidential Decision (NSPD 1), promulgated on March 5, 2001, President Bush emphasized that national security also depends on America's opportunity to prosper in the world economy. Indeed, cybersecurity lies at the core of our economic prosperity, which is our "nerve center"—and President Bush and his team should be congratulated for having taking new steps on this front.

As both Congress and the Executive branch consider how best to proceed in this area, we should not be afraid to wipe the slate clean and review the matter with fresh eyes. To this end, we should ask: What has worked to date? What has not? What are the gaps and shortfalls in our current policies? Though it is crucial to conduct our review with a critical eye, it is equally important to adopt a balanced viewpoint—one that appreciates both how far we have come and how far we have to go.

Fortunately, centers of excellence do exist—both in government and the private sector—and we should leverage and build on them. Only now, with the requisite amount of water under the proverbial bridge, have we amassed sufficient knowledge and experience to formulate the contours of a comprehensive

cybersecurity strategy. It is essential that ny strategy encompasses prevention, preparedness and incident response, vis-à-vis the public and private sectors, as well as the interface between them.

Such a strategy would generate synergies and result in the whole amounting to more than simply the sum of the parts (which is not presently the case). Such an approach would also offer enhanced protection for the "nerve center" that is the U.S. economy.

A BRIEF SNAPSHOT

Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Along with the clear rewards come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders.

Unfortunately, our ability to network has far outpaced our ability to protect networks. Though the myth persists that the United States has not been invaded since 1812, invasion through cyberspace is now a daily occurrence. There is no shortage of examples of our vulnerability, based on past red team exercises. Likewise, demonstrated capabilities—fortunately, without truly nefarious intent—are also in evidence. Already, we have seen a young man in Sweden disable portions of the emergency 911 system in Southern Florida, and a Massachusetts teenager disable communications to an aviation control tower.

Fortunately, however, we have yet to see the coupling of capabilities and intent (aside from foreign intelligence collection and surveillance), where the really bad guys exploit the real good stuff and become more techno-savvy. But, while a window of opportunity to prepare effective defenses remains for us, it will not stay open forever. It is only a matter of time before the convergence of bad guys and good stuff occurs. Clearly, we can no longer afford to rely on the two oceans that have historically protected our country. Instead, we must develop the means to mitigate risk in an electronic environment that knows no borders.

Against this background, we need a true national debate on infrastructure assurance and we need to re-think national security strategy—and, by extension, economic security and our nation's security—accordingly. It can no longer be a case of the government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses.

BUILDING A BUSINESS CASE

Cybersecurity and its implications for economic security represent twenty-first century challenges. Twentieth century approaches and institutions simply will not work. Instead, we need new organizations, novel management practices, and an array of new tools. Though this is not an area where government can go it alone, it can—and must—set a good example. In fact, only through leading by example can the government realistically hope for the private sector to commit the sort of effort—in time and resources—expected of them.

But, while government is eminently well suited to do certain things, others are best left to industry to do. Put another way, just as important as identifying what government should do, is identifying what it should not do. What follows below is an attempt to put flesh on these skeletal statements in so far as they relate to cybersecurity and its implications for economic security.

Before proceeding to focus on sector-specific (that is, public and private) strategies, however, I would like to briefly lay out a few general guiding principles. In particular, a solid approach to critical infrastructure protection and information assurance (CIPIA) must, in my view, be centered on three "prongs," namely: policy, technology, and people. Underpinning this triadic structure must be education and awareness, and superceding it must be leadership. Without leadership, the entire structure crumbles because policy priorities are only sustained if political will and the necessary resources support them.

IMPROVING THE PUBLIC SECTOR'S CIPIA READINESS

The starting point for the discussion here must surely be Presidential Decision Directive 63, the May 1998 directive that established the Clinton administration's framework for tackling the critical infrastructure/cybersecurity issue. Among other things, PDD-63 established the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Assurance Council (NIAC), as well as identifying the "National Coordinator" (at the NSC) as the central coordinating figure for the federal government. The PDD laid out aggressive goals for improving federal systems, incident warning and analysis, research and development efforts, IT security worker skills, and cooperation among federal agencies and with the private sector. As the first serious effort to address this problem, the PDD made significant improvements in the awareness of the CIPIA challenge, prodded federal agencies in to fixing their more egregious vulnerabilities, achieved some limited crosscutting federal agency improvements, and initiated a private-public dialogue on the CIPIA issue. Unfortunately, the "National Coordinator" was not always given all the requisite management and budget support necessary to enforce federal

planning efforts and, as a result, implementation of the PDD was not as comprehensive as the planning that went into it.

The Clinton administration was frequently not able to break the strong agency structures that were required to implement crosscutting programs. For example, it was often difficult to get agencies to adhere to standards or invest in systems that had significant fiscal implications. The planning, implementation and execution of an issue as complex as CIPIA is severely complicated by the fact that cybersecurity in the federal government is still strictly organized along vertical lines, both in federal agencies and in the legislative bodies that authorize and appropriate budgets. The successes that the Clinton administration enjoyed were often in areas without significant budgetary implications, or where the need for change was so compelling that some work had to be accomplished. Without strong budgetary authority residing in the National Coordinator, many important items could not be accomplished and, among other things, this made it very difficult to assess responsibility or accountability when CIPIA readiness failed.

On a positive note, the Department of Defense (DOD) and Intelligence Community have established a level of information assurance readiness that is typically much more mature then their civilian agency counterparts. This is to be expected, as they have experienced the impact of cyberattacks over the past decade and experienced many of their own vulnerabilities. The rest of the federal government will continue to benefit from these DOD experiences, and the solutions that DOD has crafted for itself.

Against this background, the Bush administration enters the issue and must quickly determine how to streamline and readjust the CIPIA readiness of the federal government, to better coordinate federal agency efforts, clarify responsibilities, reduce redundancies, and most importantly, heighten accountability.

Seven recommendations for action in the federal government follow.

1. Leadership

Critical to the federal government effort is having at its apex a single individual or group endowed with the requisite powers and responsibilities to make the system work. To this end we need to appoint a senior government official with clout or "teeth"—that is an Assistant to the President for Information Security, or a Deputy National Security Advisor—whose efforts are supported by the White House. This senior official would have a small staff and use an interagency working group to coordinate federal agency efforts and programs. This position should be confirmed by Congress and among other things would be empowered to issue directives regulating the security of federal agencies IT systems; would hold

budget review authority on those portions of a federal agencies budget concerning information technology or critical infrastructure to ensure sufficient security funds are requested; and would conduct audits/assessments so as to ensure federal agency accountability and adherence to IT security standards. This senior official would be responsible for reporting to the president, and to the Congress, on the performance of individual agencies.

In addition, this senior official would be responsible for developing an annual plan to identify crosscutting issues, have a limited budget to begin to develop crosscutting government-wide solutions, and ensure sufficient research and development efforts are undertaken.

2. Risk Mitigation

A key element in improving the computer security of federal agencies is the need to rapidly respond to incidents or threats and repair known software faults. The federal government must implement a system to provide real time information assurance vulnerability alerts to system administrators, identifying possible attack techniques or targets and known threat ISP addresses. This system, which could leverage the less robust FEDCIRC system already in-place at GSA, must be fully connected to the defense department, intelligence, and law enforcement warning systems and must also maintain good communications with private sector operated warning centers.

An equally important risk mitigation effort in the federal government is the efforts to rapidly identify, distribute and install software "patches" which are developed by vendors to correct known flaws in operating system codes. The time period between the distribution of the patch by the vendor and the installation of the patch by the system administrator is the most vulnerable time for an operating system, and the pace of this installation must be increased. For now this is a manual effort and one that requires good centralized warning of patches and applicability, and equally efficient operation at the local level by the individual system administrators. Additionally, the federal government must work hard on the development of automated tools to help with both vulnerability alert distribution and automated pact identification and installation.

Finally, to evaluate the effectiveness of the security management and risk mitigation efforts at federal agencies, the central office or board could have an "expert review team" at its disposal. This "red team" of 20-25 personnel with the requisite technical skills, could be used to evaluate the cybersecurity over federal agencies and provide feedback (government-wide) on the "best practices" and common vulnerabilities they encountered.

3. Warning

A critical step towards coordinating federal agency readiness and preparedness efforts is the construction of a centralized intrusion detection and warning center. Again, the FEDCIRC system could serve as a basis for this system, but would require significant increases in personnel, and budgetary and policy authority. This center would serve a number of critical functions; it would provide indications and warning of an impending attack for all federal agencies; it would employ a federal agency "infocon" system to establish readiness and preparedness levels on federal agency information systems; it would house a cyber-incident response team to assist agencies in incident management; and finally the center could play a crucial role in the implementation of information assurance vulnerability alerts and software patch alerts mentioned previously. This center would serve non-DOD federal agencies, and would work with and parallel the efforts of the Joint Task Force Computer Network Operations that DOD has successfully employed for the past three years.

4. Standards

The federal government needs to improve its standards in both the management of information security systems and the procurement of information technology systems. In the area of security standards management, federal agencies have requirements established in numerous documents including OMB Circular A-130 and several laws. The missing ingredient has been a strict auditing and assessment system to enforce these standards. Specifically, OMB has never been properly manned to implement and enforce such an assessment system. Frequent audits by GAO have demonstrated that in the absence of a tool to hold them accountable, federal agencies have routinely failed to meet the standards laid out in A-130. If the senior official called for above is given some budgetary review over agencies IT programs, he will have the tool to enforce audit and assessment findings, which would be conducted by the "red team" mentioned above. It would also be beneficial if the results of the audits were provided to the president and Congress as a "report card" to help keep the pressure on federal agencies' senior leadership. In the absence of this pressure, many agencies do not treat information security as a critical or core agency mission.

Information technology system procurement standards are another key public sector shortfall. The government needs to have (or work with) a laboratory in which IT products undergo a review and validation process, from which GSA will then provide a list of acceptable products for federal agencies to procure. In the absence of such a procurement standard many federal agencies continue to install information technology equipment with little or no security components installed.

5. Training and Education

There are numerous components of information assurance training and education that the federal government must continue to push. First, the public sector needs to raise IT security awareness among the general federal workforce. This includes the use of effective security techniques (i.e., passwords) and the need to limit access to IT systems without proper clearance. This awareness training needs to be conducted on a recurring basis, and be tied to an employee's computer access. Second, we need to continue to train and certify our federal IT security workforce, and to the extent that this mission is out-sourced, ensure that the contractor workforce meets the proper training and certification standards for operating federal systems. Fortunately these training and certification programs are easily available in the private sector, and require very little tailoring for federal government use.

Third, we need to continue to recruit and develop a skilled and "current" IT security management workforce. While IT security managers compose only a small percentage of our federal workforce, these specialists are a rare group of worker and one in great demand in the private sector as well. The Clinton administration's "Cyber Corps" program was a step in the right direction, identifying and developing university information assurance programs, and recruiting students directly from those few existing programs with scholarships for federal service. An unexpected challenge has been the small number of existing information assurance programs, and the even smaller number of students who were U.S. nationals and thus available for security clearances and federal service. Efforts to develop academic programs, and grow a generation of faculty, need to be closely coordinated between the government, universities, and the private sector, as all three will ultimately benefit from its success.

To retain a trained and educated IT security workforce the federal government will have to evaluate its retention and pay packages, for these workers are in heavy demand outside the government as well. We need to introduce reward programs that would not only lay out a promotion path, but also establish recognition mechanisms separate from promotion (as was done in Y2K), and we need to revisit the pay scales for these relatively rare but highly prized information security experts.

6. Reconstitution

One area where little headway has been made is the effort to identify public sector information systems, and determine how they will be rapidly reconstituted following a successful cyberattack. This involves not just the federal systems that support our core agency missions, but also the private sector communication and

power systems on which the federal systems depend as well. This reconstitution effort raises challenging questions of public–private sector cooperation and coordination that will involve the Defense Production Act and similar legislation. This effort may also identify single points of failure and needed remedies that could have significant budget implications; as such, a more aggressive attempt to tackle the reconstitution problem is warranted.

7. Research and Development

The federal government is only a small player in the development of next generation information technology systems. However, in the area of information security systems the work at the DOE Labs and DARPA is still the cutting edge effort. As such, the public sector's R&D efforts are crucial to developing the "next generation" of IT system security, and we must continue to ensure that the DOE and DOD budgets provide a healthy environment for the labs to work in. Additionally, the NSF funds much of the university-based IT research that is looking at the "generation after next" and can therefore impact the consideration of security in those systems

THE PRIVATE SECTOR: A CRUCIAL NEW PARTNER

The benefits from improving the CIPIA readiness of the private sector are two-fold. First we improve the resilience of our economic infrastructure to cyberattacks and second, we improve our federal government's readiness, because so many of our governments critical functions are conducted on privately owned and operated telecommunication, information, and power systems.

Several important steps can be made by the government to support the private sector's CIPIA efforts.

1. Encouraging Standards

Government can—and should—also provide specific incentives to the private sector to better protect its own systems. For instance, government could act as the catalyst for the establishment of industry-wide standards for information assurance in different business sectors, and could establish liability limits against disruption of service for companies using security "best practices." Equally, tax breaks or equivalent "credits" could be accorded to companies that use certified safety products and enforce specific types of security procedures. (The mechanism for certifying the safety and effectiveness of security products should be the consensus product of a private-sector dialogue that government should facilitate).

2. Information Sharing

Government could also grant relief from specific provisions of antitrust laws to companies that share information related specifically to vulnerabilities or threats. Notably, the Freedom of Information Act (FOIA) has been a significant obstacle to public-private information sharing to date because companies run the risk of having sensitive or proprietary data compromised if it is revealed to the public, and fear damage to shareholder confidence if vulnerabilities are publicly acknowledged. Fortunately, FOIA-related obstacles are now being recognized and addressed. Senator Bennett (R-UT) in particular, should be commended for his leadership in this area.

3. Liability Relief

Furthermore, government could provide extraordinary liability relief to the private sector in the case of cyberwarfare (similar to the indemnification authorities set up in the case of destruction of commercial assets through conventional warfare). Financial relief for digital disasters would have insurance companies insuring to a certain level, with government intervening in cases of massive outages or shutdowns. Likewise, a consortium of insurance, software, and hardware companies could create a pool for reinsurance purposes.

Although quantifying risk in the cyber-area is difficult because of the lack of experience and actuarial data, insurance companies should be encouraged to include in their portfolios limited liability indemnification policies against cyber-disruption. Here, government should be the catalyst, not the enforcer, for the creation of parameters and standards.

4. Partnering with Federal Government

In addition to "incentivizing" the private sector in the ways outlined above, government should seek to solidify partnerships between the public and private sectors. Already, under the auspices of the CIAO, the Partnership for Critical Infrastructure Security has brought together hundreds of leading corporations and various federal agencies to address the problems of infrastructure assurance. This is a good example of a step in the right direction—but we need to do more.

By way of illustration, we should try to improve public-private cooperation through information sharing on: vulnerabilities, warnings of ongoing attacks or threats, hacker modus operandi, and solutions and defenses to established threats and attacks. In doing so, we should try to learn from our experience with the National Infrastructure Protection Center (NIPC), which was not always successfully viewed as the entry point for private sector cooperation with the

government. Looking to the future, we should aim to leverage the NIPC's strengths, its ability to conduct complex cyber-incident investigations and enforcement. At the end of the day, the NIPC, as an initiative, represents a good start—as a central focus for law enforcement and incident analysis, but not the central point for all forms of private sector cooperation.

Cross-sector cooperation on information sharing is especially important because each sector has its own comparative advantage: whereas government possesses the core insights on CIP from a national security perspective, the private sector possesses the core insights on information security management. With this in mind, government should continue to assist the private sector by interacting constructively with information sharing and analysis centers (ISACs), which are sector-specific associations on the industry side, and by continuing to facilitate cybersecurity discussions within these various sectors (including banking and finance, telecommunications, and information technology).

KEY ISSUES AND CHALLENGES

The suggestions above are not exhaustive, of course. And, even if it were possible to cover the field, it must be conceded that no matter how concerted our efforts are, there will be failures, whether in the public or the private realm. For this reason, the reconstitution issue (that is, the restoration of essential systems and services) is a matter that we cannot afford to ignore. Indeed, continuity of operations and government may be the key to deterrence: if we can restore our systems and provide business continuity in relatively short order following an attack, the incentive to engage in further attacks of the same sort in future should be diminished.

Our policies in response to threats of any kind, moreover, must not stifle the engines of innovation that drive our economy and enhance our lives. We cannot afford to overreact or put up too many virtual or physical walls. Indeed, the worst possible victory granted cyberattackers would be one that compromised our precious, hard-won rights and values, leaving our society less open, less tolerant, and less free. Put another way, it simply makes no sense to infringe upon civil liberties in order to preserve them.

In particular, some seem to think that privacy, security, and electronic commerce are mutually exclusive. This is just not so. The "game" is not zero-sum: we can—and should—ensure privacy, security, *and* e-commerce. Indeed, it would be fair to state that you cannot have privacy without security, and without security, e-commerce will never flourish.

Plainly, the challenges that we face are great. But we, as a nation, are up to the task. At the end of the day, it all comes down to leadership—not only in government, but in the private sector and on the part of individuals, too. Critically, the president and Congress must demonstrate political will on this matter. But that alone will not be enough. We all share responsibility for this issue and we must all muster the will, and be prepared to contribute the resources, to deal with it.

Mark Montgomery is a surface warfare officer in the United States Navy. He is currently assigned as the first Commanding Officer of the USS McCAMPBELL (DDG 85), a guided missile destroyer being built in Bath, Maine.

From 1998 to 2000 he served as Director for Transnational Threats at the National Security Council, where he worked in the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. He helped to coordinate national security policy in the areas of information warfare, counter-terrorism, and information security training.

From 1988 to 1998 he served in a number of shipboard assignments, including USS BAINBRIDGE (CGN 25), USS LEFTWICH (DD 984) as Operations Officer, USS THEODORE ROOSEVELT (CVN 71), as Reactor Electrical Assistant, and most recently as Executive Officer on the USS ELLIOT (DD 967).

A resident of Sunapee, New Hampshire, Commander Montgomery graduated from the University of Pennsylvania receiving B.A. and M.A. degrees in History and Political Science, and was commissioned in the U.S. Navy through the NROTC program. He subsequently attended Oxford University, where he earned a Master's in Modern History. He has also completed the naval nuclear propulsion program.

National Security in Transformation: Outlining a Comprehensive Approach to National Information Power

By William Gravell

One of the most important public-policy developments of the past decade has been the emergence of the related disciplines of information assurance (IA) and critical infrastructure protection (CIP) at the national level. An impressive body of good work has occurred in the field of IA/CIP in recent years, including this set of reports. Taken together, it all serves to demonstrate that leading authorities in many fields are moving towards a consensus regarding at least some of the Information Age threats before us. The built-in preconceptions of both government and industry, naturally derived from their historic relationships in dealing with each other, have begun to give way in the face of the need to collaborate for mutual benefit. Most notably, the issue has spanned the divide between the Clinton and Bush administrations, avoiding politicization for the most part. The thoughtful advances being enjoyed by IA and CIP in higher education and the legislative process are noted with gratification. Another very encouraging sign is found in the growth of the population of articulate and confident professional "IA/CIP practitioners," both in and out of government. The subject is rapidly working its way down the hierarchical structure of organizations to the true working level, and broadening to penetrate almost all corners of at least the federal executive branch. Today, few would seriously dispute the status and acceptance of IA/CIP as a legitimate and important national policy topic.

All of this represents genuine—and genuinely commendable—progress. The policy, legislative, technological, and behavioral modifications sought in this area are almost all proper and needed. We may be hopeful that the reviews, checks, and balances built into the public policy process will eventually "polish out" whatever burrs remain.

SO, WHAT'S THE PROBLEM?

All of the foregoing "feel-good" reporting relates to the current state of play of various efforts to deal with vulnerabilities of the domestic national information base and the infrastructures upon which our society is dependent. Today, while much remains to be done, that particular field is positively crowded with eager participants and well-intended projects. At this point and increasingly hereafter,

IA/CIP is a domain more attractive to the skills of the systems engineer than the political scientist or national security theorist. And yet, for all of that, one cannot help feeling that all of these efforts, energetic as they are and successful as they may become, fall short of the real national need, and especially the opportunity uniquely available to a country like ours in these times.

One hears today that IA/CIP is a component of national security, and demands attention appropriate to that status—fair enough. The real question is, what else should be enfolded within the national security envelope that is similar in its technological nature, if not necessarily its defensive character, to CIP? Is a "CIP strategy," standing alone, viable—much less optimal—as an expression of the nation's objectives regarding the salient features of the Information Age? Is it resonant with other aspects of the nation's total approach to achieving its global policy aims?

No protection can be perfect, and no attack should be permitted to pass without a response, measured for its appropriateness in consideration of the transgression, target, and actor. However, it is exactly these processes which are most visibly deficient in our current national legal, technological, and policy structure related to IA and CIP.

The essential point of this paper is the assertion that the issues exposed by these questions may only be fully illuminated when total defensive efforts related to information are seen in the context of a larger strategy. Reduced to the simplest level, this suggests that the achievement of a comprehensive, viable domestic information-protection capability is a "means" to an even larger, more complex, and (even) more abstract set of "ends," within which a workable national CIP regime is a necessary but insufficient capability.

In 1998, this author wrote an article, which was eventually published in the Duke University Journal of Comparative and International Law. The piece devoted most of its space to a discussion of the progress of IA/CIP efforts to that time, but also tabled a concept and coined a term—"National Information Power."[1] The article advocated pursuit of such a "capability" as a national objective.

The most obvious and immediate question is, why bother to take on a project of such an obviously difficult nature? Is such an undertaking needed, or even a good idea? This question may be addressed in terms of both the "stick" and "carrot" forms of motivation. In the first case, the threat to our nation and its institutions is real, increasingly visible to even the most steadfast skeptics, and growing at exponential rates. It is this reality, above all, which has fueled the enormous increase in attention to information protection discussed briefly above, and elsewhere in this report. No protection can be perfect, and no attack should be

permitted to pass without a response, measured for its appropriateness in consideration of the transgression, target, and actor. However, it is exactly these processes which are most visibly deficient—or lacking altogether—in our current national legal, technological, and policy structure related to IA and CIP. Overcoming these deficiencies requires us to explore linkage of national protective strategies to such concepts as deterrence, preemption, and retaliation, and we will do so, later in this article.

On the positive, or "carrot" side of the motivational balance lie the advantages available to a nation as rich as ours in the currency of the Information Age—technology, creativity, and industry—to employ those admirable characteristics in support of the broad national policy agenda globally. These opportunities are available whether the government seeks to speak or act by itself, or on behalf of commercial interests as an agent in support of trade or other policies.

RISKS AND REQUIREMENTS

Stepping up to the next level of thinking about the eventual goals and effects of these national exertions immediately warns and informs us regarding the difficulty in managing "across the grain" of traditional organizations and equities. Even within the immediate, defense-only goals of CIP, it is easy to demonstrate the need to create workable associations between fundamentally different processes in several areas. For example, the Duke article spoke at some length about the relationship of cognitive intelligence "indications" to the dissemination of "warning," a mechanistic communications activity guided by a specific rule set. This pairing creates "I&W," and although the requirement for such a capability in the pursuit of any meaningful national CIP effort is well documented, the creation of a viable, broadly-based I&W structure predicated on IA/CIP has eluded us to date. How much more difficult will it be to horizontally integrate processes where neither the rationale nor implementation can draw upon historic models, or at least not models within the personal experience of the current participants?

It is reasonable to conclude that the difficulties inherent in this example will be magnified many times when we seek a context for the purely-protective goals and programs of CIP within the totality of our national interaction with friends and enemies, at home and abroad, in all the areas touched by "information." Clearly, this interactive, horizontally integrated view requires a holistic appreciation, if for no other reason than to establish convincingly that the end benefits will justify the efforts required to reach them.

THE OPPORTUNITY

If we accept this requirement to be able to perceive, describe, and defend the *end state*, then the need for a *strategy*, as a way to organize the pursuit of that goal outcome, must follow. It is this, above all, which the nation lacks today. Absent *both* an end state and a strategy, we cannot be sure any given current effort is proceeding efficiently toward definable and optimal goals; we will have difficulty ordering relationships between activities in parallel and in series related to long-term goals; and we won't know when, where, or in what condition we may hope to achieve a relatively "steady state" capability.

All the work to date in wrestling national CIP to the ground has some flavor of strategy, and is getting better all the time in that regard. However, no knowledgeable practitioner today would defend the suggestion that such efforts look upward and anticipate a larger and more complex construct, within which a comprehensive protective regime is but one component of the total *integrated* capability required.

The "end state" envisioned is one in which "information power" is recognized as a permanent and measurable aspect of total national strength, alongside the more classic components of economic, military, political, and diplomatic power. In one sense, this represents little more than the appreciation that "information," while often abstract and featureless, has real power in many applications. Closely related to this, a comprehensive "national information strategy" must be created, which must necessarily support a broad range of measures to *positively support* national policy goals. At the same time, and in a balanced way, this strategy must *also* seek to "defend" some defined and bounded set of information equities, deliberately culled from the vast body of "information" that surrounds our daily lives, now and increasingly in the future. Efforts to create and implement such a strategy must recognize that the whole enterprise plays out on a global scale, on an open-ended timeline, and in a highly dynamic environment. Therefore, the "end state" of this strategic effort would be the ability to attain, sustain, and execute a new force for our national needs in these times: "National Information Power."

As noted at the beginning of this discussion, the Duke piece made reference to National Information Power (NIP) and the need for a strategy to approach it. Unfortunately, those ideas were only cursorily treated with in an article primarily pointed in other directions. However, since IA and CIP seem to be doing well enough on their own these days, we may now briefly step up to the next level. From that vantage point, we will offer some answers to questions not yet being widely asked. These issues must be addressed, however, if we are to ever realize the full return available from our current and future national investment in CIP.

THE ESSENCE OF NATIONAL INFORMATION POWER

The fundamental bases of National Information Power (NIP) and its supporting strategy are considered to be *balance* and *breadth*.

National and other efforts to achieve IA/CIP capability weight the scales in one dimension. However, viewed in isolation, these processes and technologies can be seen as both passive and reactive, surrendering initiative to adversaries of every description. Offsetting and *balancing* that domestic and protective capability, American leadership has the opportunity to link it to the means of *deterring* aggression, *projecting* national will—punitively and destructively if necessary—and actively *advancing* our policy goals globally. The specific basis for linkage in policy will be outlined below. For now, the key points are that by restoring balance to the total environment of "information explicitly associated with national security," we strengthen the hand of our leadership by expanding its options, while enhancing strategic stability. Beyond that, the positive opportunities to advance the broad national agenda in an information-rich (and dependent) world economic, political, and security environment are attractive, and deserve to be explored.

As noted and generally understood, "information" is a pervasive aspect of modern life. It is clear that no organization or authority—governmental or otherwise—will succeed in "controlling" anything more than a tiny fraction of the information that surrounds us. Consequently, we must face the decision of whether we wish to pursue breadth *or* depth in our understanding and active management of "our" information, knowing that we cannot have both.

The answer is clear—we must pursue the *broadest* possible visibility and topical exposure, in order to gain visibility into new areas of potential initiative, while reducing the danger of strategic surprise. In practice, this will require the creation of a governmental strategy that addresses itself not just to the technologies, security concerns, and social conditions of today, but also looks forward in science, research, education, and related disciplines not always recognized as requiring attention in the name of "national security."

The other alternative, "deep and narrow," leaves the nation and its leadership well prepared to deal with a certain class of scenarios, but with only limited ability to respond to many contingencies that fall outside that area of interest. In the worst case, this may also foster development of a strategic "blind spot" that could leave us vulnerable to serious exploitation or even attack. If it were obvious that our government, and thus presumably our national interests, were so narrowly directed, our adversaries would enjoy significant advantage, and hold the initiative in many cases.

COMPONENTS OF NATIONAL INFORMATION POWER; ELEMENTS OF NATIONAL INFORMATION STRATEGY

The perceived benefits of a balanced approach to NIP were briefly outlined above. Beyond those, there is an even more basic reason for linking these processes and equities within a common framework. Namely, each is made more powerful and viable in the process.

Defense of information must be a daunting, even impossible task, without some sense of boundaries. Defining those boundaries requires an organizing principle. What is the legitimate *scope* of *government's* engagement in the protection of information equities it does not own? To what *extent* should these protections be extended? Based on, or responsive to, what threats or other concerns?[2] If one were to attempt some kind of sorting process, on what basis would any given equity be included or excluded from protective attentions? To date, no workable basis in law or policy has been created to answer any of these questions, except in the most limited sense.

It should be possible to identify those informational entities, equities, technologies, and processes of core importance to national security, based on their criticality, and their liability to access and influence. Although seen as possible, this task will be difficult, and attended by risks of several kinds—so much so that the only reason to try it at all would be the urgent necessity. Throughout this process, the goal would be to identify the nation's "vital national informational interests," with that extremely meaningful characterization being attached to the issues so selected. Intuitively, there would remain a very large mass of informational equities, some quite important to some people or organizations, and perhaps even to government itself, which would fail to "make the cut." However, the all-important test remains: Would the United States be willing to use all its power, in all forms, to defend these equities, even to the extent of going to war to do so?

Policy declarations would be required to give full meaning to that list. These must represent the unambiguous, public, and authoritative identification by the United States government of that subset of America's vital national interests which particularly resonate with the values and priorities of the Information Age, *and* which have not been so clearly identified historically. Such a declaration does nothing, in and of itself, to improve the protective posture of any underlying equity. It does, however, link violations of those specified issues to the whole range of national retaliatory responses. Moreover, it provides the opportunity to establish in policy a position that has been lacking to date in our domestic legal approach to information attack. Namely, it would allow us to define practicable distinctions between inconsequential probes and serious attacks, for the benefit both of measuring *and* of organizing our response.

Deterrence is an ancient process that has been employed many times over the years. In all cases, however, it requires that the deterring power credibly demonstrate that it possesses some terrible capability; that it will use it under a stated set of circumstances; and that in so doing, it stands to threaten something of great value to the one being deterred. It is generally, but not necessarily, true that the most justifiable form of deterrence—and of retaliation, if deterrence fails—has been a response in kind, hopefully with magnified effect. Extrapolating to the conditions of the Information Age of National Security, we see that "information," writ large, is both a target (for protection *and* attack) and a weapon or means to conduct such attacks. Further, we find all the social and technological elements required to create an information-based deterrent regime, but the necessary associations (i.e., policy and strategy) are largely absent. That is, we understand that like ourselves, many nations today, and ever more over time, are heavily dependent upon information-based processes. Any viable threat pointed at those necessary technologies and processes must be taken very seriously. And yet, for lack of a comprehensive policy framework to guide and measure our response, we endure "attacks" from nations (and others), some of which *have* declared their intent to develop information-attack weapons. The absence of the overt policy framework required to constitute a deterrence regime associated with informational equities and attack tools is judged to actually be destabilizing, as regards the global use of such tools and weapons.

As with all other forms of deterrence and all other aspects of national power, the response will be studied and applied situationally. However, by embracing this approach, national leadership will enjoy a broader, and perhaps also more morally justifiable, set of options from which to choose.

Offensive capabilities associated with the technologies of the Information Age are generally spoken of in hushed tones, if at all. Any discussion of the nature, modality or any other details regarding these "black arts" falls well outside the scope of this paper. And yet, in general terms, we cannot escape the understanding that we are talking about the recognition and institutionalization of new forms of power unique to the Information Age. We are describing the values and equities of our society, the role of government in protecting those common treasures, the capability—even responsibility—of government to enforce those protective declarations against "all enemies, foreign and domestic," and the need to hold opponent's values at risk in order to do so, *all* in "informational" terms. Does it not follow logically that in many cases today, and ever more in the future, the opposing equities and values being placed at risk will be fundamentally "informational" in nature, just as the equities we undertake to protect are? From there it is a short step to the recognition that the *validity* of the deterrent structure would be most benefitted if it included avowed abilities to respond directly, proportionately and in kind. At the same time, the *effectiveness* of the deterrent

regime would be enhanced by the known ability—and willingness—of the deterring nation to directly attack the informational core values of current and future opponents.

The conclusion is irresistible. It must be possible, and would certainly be beneficial, to acknowledge the need for "information weapons," as part of a balanced strategy of offensive and defensive capabilities, contributing to deterrence, and still preserve the vital security upon which the effectiveness of any such capability must depend. The benefits of such a move would be broad, immediate, and specific. The national advantage associated with such an initiative would be the ability to manage, at least initially, the resultant international debate.

PUTTING IT ALL TOGETHER

In the end, we see all the major elements of the proposed balanced National Information Strategy, the linkages that serve to identify the required elements, and also the gross nature of the relationships between them.

- We seek to defend our society, but government's responsibilities and rights in that regard must be understood as being limited, both in order to be acceptable in concept and practicable in execution.

- Those specifically selected equities underlying our focused defensive efforts must be explicitly acknowledged by national leadership in order to differentiate them for purposes of "national security" interest.

- Those declaratory policies gain greater strength and credibility when linked to deterrent regimes optimized for the information-based social values of today and the future.

- The general acknowledgment of powerful tools tailored to enforcement of those deterrent policies enhances their credibility, and represents a "big stick" in the event that deterrence fails and aggression must be responded to.

WHAT'S NEXT?

The short length and narrow limits of this paper only permits this brief discussion at this time. However, it must be noted, at least in passing, that there are logical constructs within which "information in national security," writ large, must be considered which are even more expansive than the National Information Strategy advocated here. The term "Homeland Defense" (HD) is currently evolving from an abstract descriptive expression into a proper noun. Its scope—domestic and

protective—is implicit in the title. . . so far, so good. What types of threats should we undertake to defend against under this banner? Here, opinions vary: missile defense, cyber, chemical, biological, nuclear/radiological, and "classic" terror threats all have some claim to consideration. Some might even offer more candidates. One thing that is clear, however, is that however many constituent disciplines or threat categories we include within HD, and whichever they may be, they have historically tended to be managed and developed in isolation of each other, as independent, "stovepiped" activities. Overcoming those barriers of organization and process will be easily as difficult as anything proposed herein regarding "information." Even so, we must acknowledge that "information" is the organizing principle around which horizontal integration of these elements must eventually be achieved. As such, the case for proceeding with speed and conviction to address and embrace National Information Power is all the more compelling.

William Gravell graduated from the United States Naval Academy and was commissioned an Ensign in the United States Navy in 1973. For the next 26 years, he served in increasingly responsible command and staff assignments all over the world, primarily as a naval cryptologic officer, rising to the rank of Captain. Highlights of his service included leadership of two signals intelligence intercept stations, and extensive involvement in the professional field now referred to as Information Operations.

Mr. Gravell's experience in Information Operations spans more than 20 years and encompasses information exploitation, protection, and attack; in aspects of business, policy, and program management, as well as tactical military and intelligence operations. While serving as the first Chief of the Joint Staff Information Warfare/Information Assurance Division (J6K), he played a pioneering role in national Information Assurance and Critical Infrastructure Protection (IA/CIP) efforts, including leadership positions on several U.S. and international policy and strategy groups.

In 1999, Mr. Gravell joined the TRW Corporation, where he now serves as the Director of IA and CIP. He is also extensively involved in numerous study and analytic efforts sponsored by government, industry, and academia, examining the imperatives and opportunities of the Information Age in technology, strategy, and commerce.
Mr. Gravell has been published in legal, professional, and technical journals, and represents TRW on the Industry Executives Subcommittee of the President's National Security Telecommunications Advisory Committee. He has served on several task forces of the Defense Science Board related to various aspects of Intelligence and Information Operations. He is a member of the Adjunct Faculty of the National Defense University School of Information Warfare and Strategy, and has lectured at all military service war colleges. He is also an Adjunct Fellow of the Potomac Institute for Policy Studies.

Notes:

1. "Some Observations Along the Road to National Information Power," *Duke Journal of Comparative and International Law*, Volume 9, number 2, at 401. Available online at www.law.duke.edu/journals/djcil/ (back issues – Spring 1999).
2. Ibid.

Cyber Early Warning: Implications for Business Productivity and Economic Security

By David Keyes

TECHNOLOGY, PRODUCTIVITY, AND ECONOMIC SECURITY

Like nowhere else of its scale in the world, the United States has a foundation of ubiquitous, reliable, and inexpensive infrastructures, including telecommunications and electrical power. These infrastructures uniquely positioned the American business community to seize upon the benefits of advances in information technology and powerful enterprise resource planning tools to achieve significant cost advantages over foreign competitors. U.S. manufacturers and their suppliers and distributors have established information system links to lower costs through vastly-improved supply chain management. Back office functions benefit from direct linkages to other businesses. Resource management applications have streamlined expensive personnel processes. The resulting growth in business profitability helped—or even fueled—an unprecedented period of economic prosperity in America. Governments at all levels have also embraced the cost and efficiency benefits of these technology innovations.

But as these new technologies began to supplant less efficient commercial and government business practices, at some point in this information technology revolution, our society crossed the line from merely benefitting from these new electronic tools to being totally dependent on them. This transition occurred largely without government intervention or oversight, despite the fact that the profitability and viability of many businesses, the economic strength of the nation, and basic government services have become dependent upon the reliable operation of these complex networks.

Whether from the standpoint of the productivity of an individual business, an industry, or our national economic security, these technologies also arguably represent one of our greatest economic strengths and our most vulnerable economic infrastructure weakness. As we learned from the Year 2000 (Y2K) problem, interconnected systems control the nation's businesses and supporting processes and infrastructures to the extent that the profitability—and even viability—of businesses are quickly placed at risk when systems fail. Thus, national economic well-being, not just national defense, must include a focus on how our critical business processes and their supporting infrastructures can be protected from electronic attack, manipulation, or exploitation.

It is within this context that the issue of cybersecurity has a growing impact on both public and private planners. Each day brings new news of automated virus tools, denial-of-service attacks, IP spoofing, trojans, keystroke capture, password crackers, logic bombs, and other attack tools that are readily available on the Internet. Because of the automated nature of many such tools, there is often no appreciable technical competence required to use them. While statistics vary, the cost to businesses victimized by such tools is growing. Increasingly, business risk decisions will ignore cybersecurity at the peril of business reputation, liability, profitability, and/or viability.

HISTORICAL EARLY WARNING MODELS

From July 1996 to October 1997, General Robert T. (Tom) Marsh, USAF (retired), chaired the President's Commission on Critical Infrastructure Protection (PCCIP). The Marsh commission report, now nearly four years old, remains the definitive public policy review of the business, economic, and defense implications of cyber-security risks, vulnerabilities, and threats. Because the report reflects the influence and views of some 6,000 individuals, groups or organizations contacted through nationwide public hearings or other means, not all the topics examined could be addressed in the final, distilled report. Among the many issues the PCCIP reviewed was the extent to which traditional national defense doctrine might have value in the world of cyber-attacks and defenses. This was one of the reviews in which I participated during my tenure as a Commissioner.

A cyberattack can originate from any part of the globe and from any nation, group or individual. The low cost of equipment, the readily available technology and cybertools, and the otherwise modest resources needed to mount a cyberattack makes it impossible for governments, much less businesses, to identify or track all potential cyber-adversaries.

Central to national defense doctrine of the last half-century has been the need for reliable, credible systems to warn of an impending attack. With the lessons of Pearl Harbor still hauntingly vivid, post-World War II U.S. leaders invested heavily in technologies to prevent any future surprise attack. The age of nuclear weapons, borne by increasingly sophisticated generations of intercontinental bombers and land or submarine-launched missiles, spurred huge U.S. investments to develop Early Warning (EW) systems and response mechanisms.

One of the most critical success factors of the historical U.S. EW process has been the blending of technology outputs with a rigorous analytical process. Huge research and development investments have created national EW systems that are

capable of detecting tangible things: they "see" the mobilization of ships, planes, tanks, or troops; they "hear" submarines or a surge in the command and control communications necessary to mobilize and deploy forces for combat; they "sense" other tangible manifestations, such as the heat plume of a just-launched ICBM. But it is the analytical overlay of these EW outputs that provides the context for their validation.

EW capabilities have not been static. Over the years, they have had to change to meet the challenge of improved offensive capabilities of actual or potential adversary nations. Toward that end, it was first necessary to determine what needed to be "watched," "heard," or "sensed." Then, the technologies to do such monitoring had to be refined or newly developed, tested, and, when sufficiently reliable, operationally deployed. Aggressive upgrade programs were critical in adapting to new threats or capabilities. Analytical skills had to be at least equally adaptive.

One of the most crucial contributions derived from EW systems in the nuclear age has been their contribution to the process of deterring potential adversary nations. Generations of U.S. leaders have recognized that these EW technology investments are crucial to that goal. As a result, potential adversaries have the certain knowledge that a strategic attack against the U.S. or its allies will be detected in advance, thus enabling U.S. leadership to authorize massive retaliation, improve the defense posture of the United States, and/or take preemptive action.

TODAY'S EARLY WARNING MODEL AND CYBERSECURITY

In examining the virtual—versus the physical—component of cybersecurity and early warning, the parallel with our historical EW models quickly breaks down. For example, traditional defense doctrine calls for the identification of the offensive capabilities of potential adversaries. The targeting of current EW systems includes monitoring the military status and command-and-control functions of a relatively small number of potential aggressor nations. This is possible in the traditional physical environment where only nations have the financial, technological and personnel resources to mount and sustain modern warfare. (See Figure 1.)

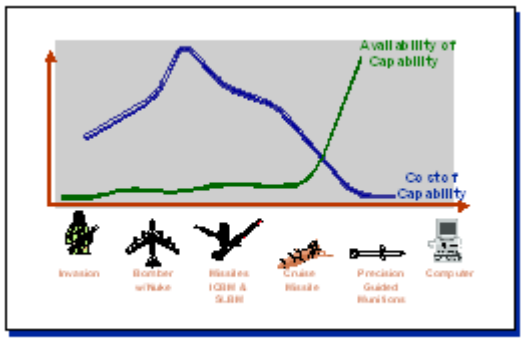


Figure 1: Cost and Availability Model

In the virtual environment, there is no one nation or group of nations to monitor—offensive cyber-capabilities are but a mouse click away for anyone with web access and hostile intentions. A cyberattack can originate from any part of the globe and from any nation, group, or individual. The low cost of equipment, the readily available technology and cybertools, and the otherwise modest resources needed to mount a cyberattack make it impossible for governments, much less businesses, to identify or track all potential cyber-adversaries.

As a second example of how the historical EW model breaks down in the cyber-world, traditional defense doctrine also calls for building countermeasures to protect against the offensive capabilities of potential adversaries. In the cyber-environment, the actual offensive capability often is based upon vulnerabilities embedded in multiple iterations of widely used software products designed with no or minimal attention to security flaws and over which governments have little, if any, control. Businesses, and particularly small businesses, often have neither the technical skills nor the resources to keep up with these security flaws and recommendations for fixing them.

As a third example of the differences in EW models, I note that in the traditional defense environment, the motivations of potential adversary nations are usually clearly demonstrated by their capabilities, their public statements, and their training and exercises. In the cyber-environment, particularly the business environment, motivation—or even determining incident causation—is much more complex. Motivations may include curiosity, challenge, adventure, malice, crime, revenge, industrial or traditional espionage, political issues half the world away, terrorism, or disruption of military capabilities. (See Figure 2.)

Figure 2: Motivations and Threat Sources

Because today's EW monitoring systems are directed at tangible things, preparations for a cyberattack would probably not be detected by national intelligence assets, thus reducing or eliminating the EW advantage normally enjoyed by the United States. As a result, without any warning and without actual physical entry, those with simple curiosity or malicious intent can deny access to critical business systems and supporting infrastructures, disrupt their operation, destroy key components, alter data, pursue illegal financial gain, and/or conduct traditional or

economic espionage. Only the federal government is charged with protecting the nation against such a breadth of threats.

In summary, while America's citizens and businesses still enjoy the protections geography provides against physical attack from abroad, perhaps without realizing it, their networked information systems lie outside traditional defense capabilities. Owners and operators of networked systems must provide for their own defense against all foreign or domestic cyber-adversaries. On a day-to-day basis, it is the system owner who must protect his or her network from acts of cyber-revenge by disgruntled insiders; theft of services, goods, or information by cybercriminals; espionage conducted by cyberspies; or disruptions caused by cyberterrorists. While the government may be able to step in after the fact to identify who might have been responsible, it is the owner who bears the burden for preventative security.

This burden is costly and often beyond the technical competence of most businesses. And in light of recent GAO reviews, it will not be surprising if many government agencies will also face challenges in establishing adequate cyber-security burdens levied by new statutes such as the Government Paperwork Elimination Act.

EARLY WARNING: DETECTING ATTACKS IN PROGRESS?

One of the purposes of EW systems and supporting analysis has been to predict preparations by a potential adversary to undertake military action. Since this predictive capability does not yet exist for cyberattacks, at least as a first step, EW may consist of detecting an attack as it begins. It is therefore critically important to know if it is possible to detect in real time whether an attack is underway. This is not as easy as some may think.

With traditional warfare, the identity of the attacker is obvious. Short of open warfare, the process gets much harder. For example, the destruction of Pan Am flight 103 required two years of extensive, globe-spanning investigation by multiple countries before the responsible parties were finally identified. It took more than a year after the destruction of TWA flight 800 to unravel the complexities of that tragedy.

Cyberattacks may be even more difficult to resolve. In the event of isolated or cascading infrastructure failures, it may not be possible to immediately establish their cause. Is the failure the result of software or hardware problems? The result of complex system interdependencies? Operator error? A virus problem? Indeed, given the complexities of present systems, and the daily challenges of keeping them in operation, the very last thought might be that a system failure is the result

of a cyberattack. Carefully prepared and cleverly done, days or weeks may pass before determining that such failures were intentionally induced. The greater the time lag, the more difficult it is to determine who was responsible. It is therefore usually not cost effective for businesses to invest in anything other than stopping "the problem" and just getting on with business.

Information Sharing as Early Warning

Our situation today holds some parallels with the discussions of the Second Continental Congress on July 4, 1776, when the delegates of the 13 American colonies approved the Declaration of Independence in Philadelphia. At that time, John Hancock warned the delegates that, "There must be no pulling different ways; We must all hang together." History tells us that Benjamin Franklin then quipped, "We must indeed all hang together, or most assuredly, we will all hang separately." In applying Mr. Franklin's point today, we must indeed all hang together to secure our interconnected information networks or most assuredly we will be individually victimized.

Figure 3: Business Drivers

Time to market is THE key imperative for many businesses, including software firms and B2C solutions providers.

Focus groups define product offerings, not security managers and customer convenience is paramount, to include low-end compatibility.

IT managers are cost centers, not profit centers, and as such, technologies that enable profitability are more sought after than security solutions for security's sake.

Business makes investments in areas that produce a competitive advantage, not in foundational infrastructures outside their control, such as utilities.

The primary e-security investments are made in the B2B space, with private networks, VPNs, and hardware and software encryption.

Unfortunately, in the cyber-environment, the federal government has left U.S. businesses to "hang separately." To date, the national response to the cybersecurity challenge has been to push for the private sector to improve its own security posture without commensurate government effort. Presidential Decision Directive 63 (PDD-63), in which I was a party to drafting, called upon government and the private sector to actualize recommendations of the PCCIP report. Specifically, it called for the creation of a series of Information Sharing and Analysis Centers (ISAC) to pool information about threats to networked systems, vulnerabilities uncovered in such systems, and information about suspicious activities or anomalous events that might indicate an attack is under way. Although investment in such things as an ISAC is outside the scope of normal business drivers (see Figure 3), multiple private sector infrastructures have agreed to accept this

challenge. The federal government, however, has not made the proportionate investment PDD-63 envisioned.

Since before PDD-63 was signed, I have been associated with the ISAC process, and most recently, in the creation of the Information Technology ISAC (IT ISAC). Although the ISACs are positive first steps, they are only baby steps and are subject to significant limitations. For example, despite private sector participation in the ISAC process, with the exception of the financial industry, there are few economic incentives for developing high-end cybersecurity solutions. In addition, the economic downturn of the last year has trimmed industry profitability and the availability of volunteer or financial resources to sustain the ISACs. At the same time, PDD-63 notwithstanding, there has been limited information contributed from the government to prime the "information-sharing pump" and almost no government funding for anything other than the worthy efforts of the Critical Infrastructure Assurance Office (CIAO).

In February 1998, the Department of Justice established the National Infrastructure Protection Center (NIPC) under a framework I had proposed in late 1997, and charged the NIPC with being a national cyber-warning center. A recent GAO report sets out its perspective of the reasons the NIPC has failed to fulfill its envisioned role. Those reasons aside, viewed solely from the perspective of the historical EW model, the NIPC has failed as an EW center because it has not combined an aggressive EW technology development program with the high-quality analytical support necessary to achieve the required level of excellence—nor has it been funded to do either. Without investment in the requisite high level of technological competence and superb analytical capabilities there will be no federal cyber-EW center worthy of the name, whether in the NIPC or elsewhere.

In addition to the NIPC, the government has invested in Intelligence Community and Department of Defense cybersecurity activities. One such example is the Joint Task Force/Computer Network Operations (JTF/CNO) of U.S. Space Command. Like the NIPC, but for other reasons, they share the failure to provide meaningful cybersecurity and EW information to the business community. Indeed, the argument can be made that Intelligence Community and Defense Department interest in information sharing is a one-way street, with them looking toward the private sector as the "trip wire" to alert the government to cyber-anomalies.

There are other important issues that concern the private sector that the government should consider as the private sector is pushed to assume more and more of the nation's cybersecurity burden. First, today's businesses, large and small, are often multinational companies with a vested interest in being good citizens in multiple countries, not just the United States.

Second, global communications are seamlessly interconnected business interests are placed at risk by the information warfare of the Department of Defense. Viewed from the business perspective, an information warfare attack in one part of today's global network has the potential for spinning out of control into the broader global communications system.

Third, the private sector believes that it, not the government, has the capability to devise cutting-edge technology solutions and the expert staff to implement those solutions. Finally, the private sector, particularly regulated industry, is suspicious of government motives when the government is "just here to help."

ADDRESSING THE OTHER DIGITAL DIVIDE

Much is said today about the digital divide—the gulf between those who do and do not have access to today's advanced information technology. But that is not the only digital divide. As a generalization, true cybersecurity protections are only available to the very large or particularly well-financed companies. In seeking to meet any national goal to eliminate the vulnerabilities inherent in the backbone networks upon which critical business processes rely, the government should step up to its responsibility to provide several things.

First, it should provide the means to protect the general cybersecurity welfare of all Americans. Next, it should provide funding for the research and development of tools to protect the electronic lanes of interstate and foreign commerce. Third, it should make material contributions to the sharing of meaningful cybersecurity information with the business community.

In providing the means to protect the general cybersecurity welfare of all Americans a different approach must be taken. If the only meaningful government cybersecurity research investments are in classified activities, the EW role of the business community will be to serve in the same roll as cheese on a mousetrap trigger—with their cyber-victimization forming the basis of the nation's alerting mechanism.

In providing funding for the research and development of tools to protect the electronic lanes of interstate and foreign commerce, the lessons of the historical EW model should be reviewed. Aggressive investment in targeted technologies and the requisite analytical skills are required for a meaningful EW process. Thereafter, investment in countermeasures to detect, prevent and neutralize threats at the network backbone will provide the next level of protection.

In the area of information sharing, government investments should be made to augment, not rely upon, private sector information sharing. Defense, intelligence,

and law enforcement cybersecurity information collection and analysis should be aggressively funded and its efficacy monitored. Toward that end, to maximize business confidence, a government-sponsored enterprise, managed as an independent corporation, should be considered to "jump start" specialization in cybersecurity issues for the overall benefit of the business community, large and small. This business-based solution center should be free to seek innovative cybersecurity solutions outside of government bureaucracy and be free from federal payroll limitations that drive most premiere technologists to the private sector.

The enterprise should have the mandate to primarily serve the cybersecurity needs of small to mid-size businesses. After five or so years, the government sponsorship should be withdrawn, forcing the enterprise to succeed in the marketplace. In the interim, specialized cybersecurity products developed at government expense, be they firewalls, intrusion detection sensors, attack signature databases, or other unclassified products, should be made available through the enterprise for private-sector exploitation. The enterprise should also be required to assist government at all levels when requested.

Such an enterprise can serve as a central ISAC for all industries or businesses that require cybersecurity information sharing support. Although likely a controversial point, it could also serve as a standards body for cybersecurity products, much like the Underwriters Laboratory.

Figure 4: Information Sharing Model

Any approach as radical as a government- sponsored enterprise will surely draw criticism from vested interests in and outside government, thus potentially dooming such an approach at the political level before it would have a chance to succeed at the functional level. If so, at a minimum, the federal government at some trusted level must begin the process of materially contributing to the private sector understanding of the nature of the cybersecurity threats and vulnerabilities it faces with information that can grow to constitute a meaningful first step toward cyber-early warning. (See Figure 4.) With that goal in mind, the government should collect and propagate information about attack tools and defenses against them. Similar information should be collected about organizations that support or sponsor harmful activities. Meaning-

ful warnings about organizations and intentions should be made available, as should information concerning federally-sponsored research and development. In turn, the private sector should shoulder the burden of protecting itself against attack tools and report to some neutral location the information about attacks it has experienced.

FINAL THOUGHTS: TOO MUCH TO ASK?

As a nation, we have embraced the information age as a means of improving our way of life and our economic prosperity. We must also commit to finding new ways of protecting and strengthening the critical cybersecurity infrastructure foundations upon which our mutual futures rely. In this environment it is not too much to expect of the government that it, not the private citizen or the business sector, should shoulder the majority of the burden envisioned in PDD-63 to be sure that the nation shall have achieved and shall maintain the ability to protect our critical infrastructures from intentional acts that would significantly diminish the ability of:

- The federal government to perform essential national security missions and to ensure the health and safety of the general public.
- 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.
- The delivery of essential telecommunications, energy, financial, and transportation services.

Operating under such a strategy will ensure that any interruptions or manipulations of these critical functions would be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Early warning of cyber-incidents is central to achieving these objectives.

David Keyes spent 27 years in federal service. At the time of his retirement, he was the Acting Director of the President's Commission on Critical Infrastructure Protection (PCCIP) and Chair of the National Infrastructure Protection Task Force. He was the first Inspector-in-Charge of FBI worldwide computer intrusion and investigations and infrastructure protection. His career included two assignments in the Executive Office of

the President. In May 2000, he was the recipient of the Armed Forces Communications and Electronics Association (AFCEA) first annual award for excellence in electronic critical infrastructure protection.

Transition between Law Enforcement and National Defense

By Scott Charney

INTRODUCTION

We are in our fourth revolution. We were hunters and gatherers, then agrarian, next industrial, and now digital. With each major revolution, society has embraced change for its obvious benefits, paying scant attention to the predicable harms that would follow. For example, the Industrial Age promised greater production and efficiency, lower cost goods, and a dramatic increase in our standard of living. Only after the Industrial Age was unleashed did society begin to focus on the other results: acid rain, sweatshops, and child labor, just to name a few.

The digital revolution has proved to be no different. The growth of the Internet has, for the most part, been fueled by its huge potential, both real and imagined. E-commerce figures prove that the Internet is bringing astounding commercial growth, with only greater rewards to follow.[1] The changes for individuals have been no less dramatic, with an ever-greater ability to engage in political discourse, find the most obscure information, and communicate with friends, family, and colleagues around the world.

In response to criminal activity—including military and economic espionage—law enforcement and national security personnel have struggled to remain effective in an increasingly complex technological world.

But like past revolutions, this one too has its darker side. Since the value of information lies in its use, the Information Age has stirred debate over the collection and use of information and the seemingly unstoppable erosion of privacy.[2] As a communications medium, the Internet allows any individual to publish globally, without the fact-checking and editorial controls normally present in traditional large-scale media outlets. Although this certainly has benefits, the fact remains that some speech crosses the line between proper and unfair (e.g., defamation), and the potential for causing damage increases with the size of the audience. And, of course, there is computer crime, a term often meant to include both hacking (computer abuse affecting the confidentiality, integrity, or availability of data) and the use of computers to facilitate traditional offenses (e.g., Internet fraud and the distribution of child pornography).

Significantly, in both civil and criminal cases, the Internet's attributes of global connectivity and lack of traceability may allow speech or action without accountability, no matter how harmful the consequences.

In response to criminal activity—including military and economic espionage—law enforcement and national security personnel have struggled to remain effective in an increasingly complex technological world. Their efforts have not been without controversy. From Clipper to Carnivore, they have been under attack from all sides: markets, civil libertarians, Congress, and the media.

As is so often the case in such passionate debates, the problem is not just the merits (which each side can claim in abundance), but also the process. Simply put, the problems posed by this revolution are too complex to be addressed as they are being done today: ad hoc and reactively. Instead, we should reassess certain fundamental assumptions about how to protect public safety and national security. Even more expansively, we should undertake a comprehensive review of the way in which we, as a society, balance the needs of commerce, law enforcement, national security, and privacy.

THE SECURITY DILEMMA

The Internet was designed as a military communications network. As such, its early users were military personnel, government defense contractors, and certain academic institutions. Simply put, in the beginning the Internet was available only to a group of trusted users, Internet crime was not a concern, and security was not critical. In the early 1980s, however, IBM came out with the personal computer and the government declared the Internet a public resource. Suddenly, everyone was able to access the Internet, and the Internet lacked security.

As the hacker attacks began, the scope of the insecurity problem became clearer. Computer networks not only had a large number of known vulnerabilities, but new vulnerabilities were being reported weekly. Studies began to confirm the scope of the problem. For example, a Computer Security Institute Survey in 1995 reported that losses from FBI-reported computer crime had already reached $2 billion dollars.[3] Another survey revealed that 98.5% of the 182 respondents indicated that their businesses had been victims of a computer-related crime, with 43.3% saying that they had been victims more than twenty-five times.[4] But even these surveys were viewed as only the tip of the iceberg; virtually all computer crime experts reasoned that most computer crimes were either not detected or, if they were, not reported.

This supposition was confirmed by a controlled study in which the United States Department of Defense attacked its own machines. Of the 38,000 machines

attacked, 24,700 (65%) were penetrated. Only 988 (4%) of the penetrated sites realized they were compromised, and only 267 (27%) of those sites reported the attack. This in an agency with mandatory reporting and a staff that recognizes the importance of following orders. Moreover, to the extent the military has long been required to protect state and military secrets, it is more security conscious than most civilian agencies and private companies.

These broad studies have been supplemented by specific cases raising concrete concerns. Hackers have attacked the confidentiality of data, stealing Defense Department information and medical data.[5] Data integrity has also been affected, sometimes noticeably (a defaced Web page), sometimes in ways meant not to be detected and therefore more dangerous (e.g., an individual hacked a courthouse, apparently in an attempt to commute his prison sentence to probation). Finally, there have been serious denial of service attacks, such as the "Morris worm," which shut down thousands of computers as far back as 1988, and the more recent distributed denial of service attacks affecting key institutions such as Yahoo and CNN.

These studies and cases have led to more advanced thinking about the risks created by our increasing dependence on information technology. With society becoming ever more dependent on computers, it is now recognized that the disruption of our networks could seriously affect national security, public safety, and economic prosperity. The disruption of power delivery, transportation services, banking and finance systems, and telecommunications systems could seriously disrupt the everyday lives of our citizens. Of greater concern is the potential for a cascading effect: how will attacks on one network lead to the failure of others? For example, if the telecommunications infrastructure is disabled, how will the banking and finance infrastructure, which relies upon telecommunications for electronic funds transfers, be affected?

The concern is not hypothetical: there has already been a "cascading effect" case. In the town of Worcester, Massachusetts, a juvenile attacked a telephone switch. In the course of the hack, the computer asked "Do you wish to reset the switch? (Y/N)." The hacker entered "Y," thus eliminating all of the custom settings of the switch and disabling phone service in the local area. A hacked phone switch, lost phone service.

But that was not all, for this switch also serviced a local airport. The tower was unmanned, and as planes approached to land they would radio the tower, which would automatically send a signal—across the telecommunications network—to activate the landing lights on the runway. As the next plane arrived, the radio signal was sent, but the disabled telephone switch prevented the landing lights from activating, and the airport had to be closed. Attack on a telecommunications

network; failure of a transportation system. In this case, it was a juvenile and a small airport. What happens when terrorists attack the phone switches responsible for O'Hare?

THE PUBLIC SAFETY/NATIONAL SECURITY CONUNDRUM

After years of debate over encryption policy, a press conference was held to announce that the United States government was substantially relaxing export controls on encryption products.[6] At the press conference, then-Deputy Secretary of Defense John Hamre made a critically important statement that was not reported by those members of the press in attendance. He said, "law enforcement is now responsible for home defense." Indeed, the world had changed.

Throughout our history, citizens have relied upon government to protect public safety and national security. But all threats are not the same, and we have created different organizations and mechanisms for addressing different threats. To protect citizens against crime, we hire, train, and equip law enforcement personnel. To protect us against those who would steal our military secrets or attack our vital state interests, we rely upon the intelligence community, both affirmatively to collect foreign intelligence, and defensively through counter-intelligence techniques. Counterintelligence techniques are also used to protect economic secrets from foreign threats.[7] Finally, to address the military threat posed by another state, we fund a military, supporting personnel, equipment and weapons. In short, depending upon the threat, we deploy a different resource, and each resource plays by its own set of rules.[8]

This traditional model works, however, only when one can identify the nature of the attack; specifically, who is attacking and for what reason. This traditional model fails in the Information Age because when computers are under attack, the "who" and "why" are unknown. By way of example, many years ago a Russian military plane shot down a Korean civilian jetliner. For a long time, notwithstanding Russian claims of non-responsibility, it was widely believed that state action, or at least rogue military action, was responsible. Why? Because civilians do not have access to fighter jets.

But the notion that only states have access to weapons of war is no longer correct, at least not if information warfare is considered. Simply put, we have distributed a technology that is far more powerful than most that are placed in the public domain. Traditional vigilance regarding states that support terrorism, political unrest, or are otherwise considered "rogue" (i.e., "nations of concern") are now supplemented by threats from "individuals of concern," a far larger pool, and one that is harder to identify and police.[9] As a result, an attack upon the Defense Department may come not only from a foreign nation conducting information

warfare, but also from juveniles on the West Coast, as it did in Solar Sunrise (the case name for a widespread attack against the U.S. Department of Defense).[10] To the extent the country detects a cyberattack but does not know who is attacking (a juvenile, a criminal, a spy, or a nation-state bent on committing information warfare), what resources should it deploy in response?

The most likely answer—at least pursuant to current thinking—is law enforcement. This is because, with few exceptions, any attack on United States' computers will violate the Computer Fraud and Abuse Act, regardless of the identity and motive of the attacker.[11] Thus, Secretary Hamre's comment about home defense. But does this "default setting" make sense, and what will be the end result if law enforcement spends months investigating a "cybercrime" only to find another country is engaging in espionage or, worse, information warfare?[12] By analogy, it would be like sending the FBI to Hawaii on December 7, 1941 to investigate a trespass by Japan. Of course, the example is absurd because in the physical world, the differences between crime, espionage, and war are often self-evident. In the cyberworld this is not so, and we must rethink how to protect ourselves from attacks even when critical decisional information is lacking.

An example may prove illuminating. Suppose the Defense Department identifies a sophisticated hacker attack in which sensitive military information is being copied from a government computers. The return address on packets transmitting the attack reveals that the immediate source is a domestic Internet Service Provider that has, appropriately, refused to provide any past traffic data or to trace future packets absent judicial process.[13] (*See* 18 U.S.C. 2703(d) [court order required to obtain records relating to a communication]; 18 U.S.C. 3121 *et seq.* [prohibiting the installation and use of a trap and trace device without a court order].) The Defense Department consults with the Justice Department, and the latter obtains the appropriate orders.

As the attack continues, the communications are traced back to an Internet site belonging to an academic institution or corporate server located in a foreign country that is hostile to the United States and has been known to conduct military and/or economic espionage against U.S. targets. It is not clear, of course, whether the attack is being conducted by an individual acting alone, or an individual or group working at the behest of the foreign government. As a result, both U.S. law enforcement and intelligence officials are reluctant to seek foreign assistance. Both are concerned that if the action is government-sponsored, seeking assistance will only serve to alert the foreign government that their spying has been detected. Moreover, the benefit of notifying the foreign government is minimal because even if the activity is deemed to be non-state-sponsored criminal activity, foreign assistance is unlikely. Thus, the more prudent approach is to monitor the hacker's

actions longer term in an effort to better determine identity, assess the strategic plan of the attacker, and determine whether other countermeasures are warranted.

That may not, however, be possible. Under the trap-and-trace statute (18 U.S.C. 3121), law enforcement may only seek an order (or, in our hypothetical, extend the existing order) if the application certifies that the "information likely to be obtained is relevant to an ongoing criminal investigation" (18 U.S.C. 3122(b)(2)). If, however, law enforcement has little intention of approaching the foreign state and further collection is primarily for intelligence purposes, seeking an extension may be improper. On the other hand, seeking intelligence orders is equally problematic as there is no solid evidence that the activity is the responsibility of an agent of a foreign power. Indeed, years ago, when the United States was gearing up for airstrikes against Iraq, the Defense Department noted a significant hack attack and was concerned, justifiably, about whether the attack was related to the impending military action. After investigation, however, it was revealed that the two attackers were juveniles in California, working with the assistance of an Israeli hacker.

This raises, of course, another difficult problem. Although law enforcement is often accused of reluctantly sharing data with intelligence agencies, the fact remains that a "foreign" attack may turn out to have a domestic source. As a result, both statutory prohibitions and law enforcement policies designed to protect the privacy of Americans must be scrupulously honored, even if intelligence agencies are deprived of seemingly critical information. At the same time, intelligence authorities are appropriately and necessarily obsessed with protecting sources and methods, and may therefore refuse to share information with law enforcement personnel, especially if the matter is viewed as one of national security. (It may be incorrect to say that law enforcement officials are not responsible for national security; in this environment, criminal investigative tools will often be used, at least initially, in matters that are later determined to be of national security.)

In sum, traditional concerns, statutory restrictions, and differing cultures all serve to hinder our nation's ability to protect our broader interests. Although these hindrances are actually healthy in some cases (we often choose to limit efficiency to protect more important values), it is not clear that the trade-offs have been reconsidered in light of technological developments. In our new environment—marked by global connectivity, an increasingly computer literate world population, and a constant lack of relevant data regarding the source of Internet-based attacks—we can no longer assume that the law enforcement/national security dilemma will arise only rarely. To the contrary, it will only increase in frequency. To the extent that our world has changed, rules designed for the past need to be reconsidered.

THE EVOLVING ROLE OF MARKETS

It would be difficult enough if this were the sole challenge facing society, but we must also reevaluate the interplay between government and industry. Almost a decade ago, when the Soviet Union collapsed, Europeans were asked how they felt about the United States being the world's sole superpower. Their response: the United States may be the only *military* superpower, but it is *economic* power that will rule the new world order.[14] This shift was not lost on the United States government, which has formally recognized that economic prosperity is key to national security.[15] Put another way, we have elevated economic and market issues to a level previously reserved for matters such as nuclear proliferation. Expanding the government's sphere of concern in this way certainly has implications for government-industry relations, not the least of which is determining how responsibility and control of the nation's critical infrastructures should be shared.

In the past, the government's role and responsibility was more clearly defined: the government was tasked with protecting public safety and national security, using funds collected from citizens through taxation. Although it of course promoted economic prosperity as well, its efforts in this area did not require sacrificing other vital interests. In this classical model, industry was—like any person or entity—a potential victim, with its primary concern the prevention and detection of white-collar offenses. Clearly, a market-based approach to public safety and national security would never work, as these functions cannot be conducted on an economics based cost/benefit analysis where the key metric is "return-on-investment."

In the new digital economy, this tax-funded approach no longer dominates. The government, reluctant to regulate the Internet and risk stifling innovation, has repeatedly stated that the private sector is primarily responsible for protecting the nation's critical infrastructures. After all, the argument goes, it is the private sector that is designing, deploying, and maintaining our computer networks. Thus, the government concludes, critical infrastructure protection requires a public-private partnership, with industry in the lead.[16]

But by allowing industry to lead, the government has in large part ceded public safety and national security to markets.[17] Although such a non-regulatory approach certainly appeals to corporate America, it cannot be forgotten that these private sector entities' primary mission is not to protect public safety and national security, but to protect and increase profitability. This is not to say that public safety and national security concerns are irrelevant to the business community. In fact, attacks on their network may jeopardize customer and investor confidence and adversely affect economic performance. Moreover, most companies

genuinely possess a social conscience. But at the end of the day, supporting public safety and national security concerns must understandably be subordinate to a company's primary financial mission as it is economic suicide to operate at a loss no matter how important a capital expenditure may be to public safety. In sum, industry efforts to protect public safety, national security, and, for that matter, their own infrastructure are necessarily circumscribed by markets.[18]

CONCLUSION

As criminals gravitated to the Internet, theorists debated whether computer crime was new or merely old wine in new bottles. The answer has become clear: not only are traditional crimes more difficult to investigate in a global and anonymous Internet, but many of our laws, procedures, and organizational structures are outdated. Our inability as a society to meaningfully address major security violations will undoubtedly serve as a catalyst for change, but change itself brings its own risks. As citizens, we demand it all: privacy, free markets, public safety, and national security. Reflective of the complexity of the Internet age, however, these goals are at the same time compatible and contradictory. For example, encryption can at one moment protect privacy, support commerce, and prevent crime, yet at the next moment protect a criminal from prosecution after he has violated the privacy of others by downloading their financial information to commit fraud.

Faced with this conundrum, it is time to methodically reconsider how to balance our contradictory objectives in a data rich, sometimes anonymous environment. We must revisit our legal, economic, and social regimes, rethinking how we protect data, promote economic growth, ensure the effectiveness of law enforcement, and respond to an attack when lacking critical decisional facts. Perhaps hardest of all, we must reclaim our right to strike this balance, and not let markets dictate our choices. That may seem like a simple and sane principle, but it has drifted away. In a recent decision striking down a statute prohibiting commercial Web publishers from allowing minors to access harmful material on their sites, the Third Circuit wrote, "we are forced to recognize that, at present, due to technological limitations, there may be no other means by which harmful material on the Web may be constitutionally restricted."[19] Put another way, the court held that since technology provides no way to protect children, children may not be protected. Although cast as a technological result, technologists develop products based upon the demands of the marketplace. With all due respect to capitalism, society—and not the marketplace alone—should determine how our core values are implemented.

Scott Charney is a Principal at PricewaterhouseCoopers LLP (PwC), and leads the firm's Digital Risk Management and Forensics practice. More specifically, he and his staff help clients design and build security systems from scratch, test existing systems, respond to specific security related incidents, and assist law firms in technology related litigation (including responding to court-ordered discovery requests requiring that data be located and retrieved in scientifically acceptable ways). Mr. Charney also serves as a consulting and/or testifying expert in cases involving the Computer Fraud and Abuse Act and Economic Espionage Act.

Prior to joining PwC, Mr. Charney served as Chief of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. From 1991 to 1999, he was responsible for implementing the Justice Department's Computer Crime Initiative, which included supervising domestic and international hacker investigations. He is a co-author of the U.S. computer crime statute, the computer crime sentencing guidelines, and the original Federal Guidelines for Searching and Seizing Computers. He has also represented the United States on computer security and encryption matters at the Organization for Economic Cooperation and Development, and chaired the G8's Subgroup on High-tech Crime.

Notes:

1. According to Forrester Research, consumer may spend $3.2 trillion over the Web in 2003. See USA Today, August 23, 2000, p. 3B.
2. See generally, "The Internet, Consumers and Privacy," by Ellen Alderman and Caroline Kennedy, an earlier paper in this series and available online at www.internetpolicy.org, and Principles for Providing and Using Personal Information, available at http://www.iitf.nist.gov/documents/committee/infopol/niiprivprin_final.html.
3. Richard Power, "Current and Future Danger, A CSI Primer on Computer Crime & Information Warfare" (1995).
4. Carter, David and Katz, Andra, "A National Survey on Computer-Related and Technology Crime." See also, The Washington Times, October 25, 1995, Page B-9 (describing survey).
5. In one case, a country singer's hospital record was taken for sale to a tabloid. In another case, the search of a hacker's computer revealed over 3,000 prescription records downloaded from a local pharmacy.
6. At the risk of grossly oversimplifying a complex debate, encryption pitted law enforcement and national security personnel (who wanted to ensure continued access to the plaintext of transmitted and stored data) with high-tech businesses and privacy advocates (the former wanted to sell cryptography products globally, the latter wanted encryption widely deployed to protect privacy). For a more detailed discussion of this debate, see "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Association of Computing Machinery (ACM), June 1994 and National Research Council, "Cryptography's Role in Securing the Information Society," (1996).
7. Historically, states protected "state secrets," not economic proprietary data. In the new world order it is economic power, not military power, that rules. Thus, steps have been taken to protect proprietary information in ways previously reserved for classified information, such as passage of the Economic Espionage Act on October 11, 1996. 18 U.S.C. § 1831 *et seq*.

8. Cf. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq*. (establishing rules for wiretapping in criminal investigations) with The Foreign Intelligence Surveillance Act, ("FISA"), 50 U.S.C. § 1801 *et seq*. (establishing rules for wiretapping in counterintelligence investigations).
9. Not only have we distributed this powerful technology, but we have exacerbated matters by deploying it backwards. With most powerful technologies, we give it to adults first, and expect them to teach their children to use the technology responsibly. Automobiles and guns are just two examples. With computers, we have given children powerful technology that their parents and teachers do not understand.
10. The attack was first detected when the United States was gearing up for potential air strikes against Iraq, and appeared to be coming from the Middle East. Ultimately, the attacks were traced back to two juveniles located in Cloverdale, California.
11. Under 18 U.S.C. 1030(a)(2), whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any department or agency of the United States is guilty of a misdemeanor. This offense rises to a felony if (1) the crime was committed for purposes of commercial advantage or private financial gain; (2) the crime was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or (3) the value of the information obtained exceeds $5,000. 18 U.S.C. § 1030(c)(2)(B). Additionally, 18 U.S.C. § 1030(a)(3) prohibits trespassing in a government computer, even if information is not obtained.
12. In a case where the activity might involve espionage, parallel criminal and counterintelligence investigations can be run, but this poses its own problems. For example, certain information cannot be shared between law enforcement and the intelligence community, thus ensuring that the left hand does not know what the right hand is doing.
13. Typically, a hacker will not directly attack his victim, but rather hack through a series of machines so that ascertaining his identity is more difficult. For example, a hacker may attack site "A" and, after establishing an unauthorized account, attack "B" from "A." He will repeat this process, attacking "C" from "B." By "weaving" in this way, investigators are forced to backtrack along his trail, often one step at a time, to find the source. Significantly, even in a purely domestic case, each hacked site may be in a different district, thus requiring law enforcement to seek multiple trap-and-trace orders in an effort to follow his trail. For example, if a trap-and-trace order executed at the victim's site reveals the attacks are coming from "C," a separate order is needed in "C's" district to trace the communication back to "B." In our scenario, up to four orders might be needed (one for the victim, C, B, and A).
14. Face The Nation, Sunday, September 8, 1991. Garrick Utley, Commentator.
15. In a February 25, 1997 speech before the National Security Industrial Association, William A. Reinsch, Under Secretary Of Commerce For Export Administration, noted that "The world is clearly changing rapidly. Economic goals have become much more important to industrialized nations, turning allies into competitors. That is one reason why this administration has emphasized economic strength and global competitiveness as a critical element of national security. . . ." (Available at http://www.bxa.doc.gov/press/97/War2-25.htm).
16. See Report of the President's Commission on Critical Infrastructure Protection, available at http://www.ciao.gov/PCCIP/report_index.html.
17. The public safety argument should be intuitive since attacks on networks are themselves crimes and may have additional public safety effects (e.g., a telecommunications attack may disable 911 services). The national security argument flows as follows. Weak computer security may allow miscreants to incapacitate our critical networks—such as telecommunications, banking and finance and transportation—causing severe economic

harm. If economic security equals national security, then economic disasters caused by cybersecurity failures impair our national security.

18. Cf. The Cable Act, 47 U.S.C. § 551(h), with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq. It is also worth noting that, in today's global environment, a company's allegiance may not be to the United States, but a foreign power. In such situations we are not only ceding our national security to markets, but perhaps to a competitor or even an adversary. For example, allowing a foreign, state-owned telecommunications company (or even a privatized telecommunications company with close ties to the state) to buy a company that provides phone service to the United States Congress would provide a foreign state with the means for direct access to internal congressional communications.
19. ACLU v. Reno, 2000 U.S. App. LEXIS 14419 (3d Cir. 2000) (striking down Child Online Protection Act).

The Definition and Integration of Law Enforcement and National Defense Efforts With Regard to Critical Infrastructure Protection

By Angeline G. Chen [1]

INTRODUCTION

The information revolution and emerging technologies have undeniably affected our societal infrastructure, particularly with regard to the functioning of our economy and provision for our national security. The rapid technological advancements that enable a borderless economy also lead to an inextricable linking of the various systems and establishments that form America's critical infrastructure.

This nation, beyond all others, stands to profit and benefit most from the borderless economy, and concurrently holds the greatest capability of taming the technology so that it cannot be used against our citizenry or national security interests.

The establishment and integration of these systems creates tremendous opportunities for business, trade, convenience, efficiency, and the ability to better our lives and national economy. Our dependence on technology, however, concurrently and increasingly exposes our vulnerability to hostile threats—both domestic and international. Much has already been said and written acknowledging that cyberattacks upon America's national infrastructure could crash key computer-dependent control networks, such as electrical power grids, telecommunications systems and networks, transportation systems, and financial institutions. A deliberate and concerted attack by a party hostile to the U.S. on any one or more of these key systems, whether governmental or privately-owned, could have devastating effects.

The juxtaposition of the real and perceived threats of cyberattacks with America's dedication to preserving the civil liberties of its citizens and obligation for ensuring our country's national security gives rise to a significant number of new scenarios and challenges. Moreover, as the relevant technology continues to develop rapidly, the ability of the law to keep pace or anticipate dynamic situations is often severely stretched. Accordingly, as the two vanguard communities charged with protecting America and its citizens, both domestically and

internationally, law enforcement and national defense now find themselves in uncharted territory. Due to the nature of cyberthreats and attacks, the delineation of what laws apply, which agency has jurisdiction, and what tools or techniques are available to respond to an incident or series of events is often indistinct or ambiguous. One inevitable result of these developments will thus be the need to transition from a clear division between law enforcement and national defense efforts to a paradigm in which there is significant overlap with regard to the challenges, potential jurisdiction, impediments, and objectives for both communities.

The need to fully analyze and assess the consequences of this transition in real-time and on an ongoing basis, allowing for mid-course adjustments and corrections, is critical. The scope of the issue, the limited resources available, and the need for a unified, coherent national policy and plan to address this sea change underscores the need for synergizing our law enforcement and national defense efforts. Common sense dictates that a clear and collaborative understanding must be formed between the two communities so that the prime objectives of both, as well as the parameters of lawful action, are best achieved in a cooperative and thoughtful manner with regard to addressing the borderless economy and its implications for law enforcement, national defense, and the American people.

THE NATURE OF LAW ENFORCEMENT VERSUS NATIONAL DEFENSE

Traditionally, the lines drawn between law enforcement and national security are clear and distinct. Indeed, they are embedded deeply into the very underpinnings of our government and societal structure. The paradigm that governs the national defense community is one that fosters active, ongoing intelligence gathering. The focus is upon acquisition and analysis of that intelligence for the purpose of planning preventive action against suspected targets, as well as preserving existing sources of acquisition for ongoing observation. In direct contrast, the law enforcement community endorses a reactive paradigm that seeks to pursue suspected or identified wrongdoers within the context of information, which is primarily provided voluntarily, and prosecutorial processes that are strictly governed by rules of evidence that often belie discretionary interpretation. The focus is to target and identify suspected or actual violators of existing laws and regulations and, through the use and navigation of clearly identified processes, to bring such violators to those ends as are deemed appropriate under our domestic laws.

At first glance, it would seem that the paradigms of the two communities are widely at variance with one another. In truth, as illustrated by the progress and successes to date of such efforts as the National Infrastructure Protection Center

(NIPC), which is housed within the Federal Bureau of Investigation (FBI) and discussed further below, a tremendous capability for cooperative and joint effort has already been demonstrated. Within the context of addressing the challenges posed by a borderless economy, commitment to such interagency and public-private missions is imperative. As witnessed during the Y2K effort, when resources and information are shared to meet a common objective, a successful synergy can be achieved.

Nevertheless, there are also fundamental incompatibilities between the two communities. In order to realistically re-define the roles and relationship between them in a manner that makes sense, these incompatibilities must be acknowledged and incorporated into whatever national policy is formulated relating to the borderless economy and critical infrastructure protection.

In protecting the economic and national security of the United States, setting forth the parameters—both legal and procedural—under which the law enforcement and national defense communities may engage in such a cooperative and collaborative effort is of particular criticality. The advance of the borderless economy has assured the cessation of any clear delineation between the two previously independent communities: both must now learn how to combine and coordinate their resources, knowledge, and efforts to address a common objective: protection of America's economic and national security.

COMMONALITIES AND AREAS OF POTENTIAL SYNERGY

Common Challenges

While the most obvious objectives of the law enforcement and national defense communities differ from one another, both face many of the same conceptual obstacles in achieving their mission.

First, the technological challenges posed by the immediacy and anonymity of the electronic medium and actors who utilize it universally create significant impediments. Technology has rendered characterization of the target into a complex and resource-draining task—a crippling variable when speed (e.g., in tracing the originating source or in obtaining appropriate authorizations) is often key. In most activities of questionable intent and legality that take place in cyberspace, the identity, location, and objective of the perpetrating individual are not immediately apparent (and often undetected). The ease with which individuals can engage in illicit or questionable activity is unhampered by cost or complexity. Not only are the physical tools readily available, but the free flow and availability of data and information on the Internet also presents ample opportunity for even

the solo actor to gather explicit information on how to render harm or damage on others.

Second, the lack of a centralized database of incidents and/or working information-sharing model that allows for quick and reliable identification of activity significantly impacts the missions of both communities. The possible linkage of a single act or series of acts with a broader pattern or conspiracy is neither readily evident nor easily established. It is difficult, and often impossible, to determine whether a single intrusion or pattern of cyberattacks constitutes an act of mischief, intentionally illicit activity, domestic or foreign terrorism, economic or traditional espionage, or even some form of strategic military attack. Hackers, both amateur and sophisticated, regularly attempt to access national security systems. Numerous foreign nations—some of questionable intent or politically unstable relationships with regard to the United States—have explicitly incorporated use of cyber-methodologies and means into their military and national defense strategies, and no doubt likewise regularly engage in exercises that are designed to test the security parameters of national information and security systems.

Third, each establishment must put aside long-standing territorial mindsets and cultural beliefs in order to reach a successful partnership. Globalization further adds an entirely new dimension to the discussion, and a situation in which interagency control issues must be left behind. In addition to creating a seamless network of connections between the United States and other nations and entities—both friendly and hostile—the borderless economy likewise translates to a breakdown in the traditional boundaries between the jurisdictions of law enforcement and national defense activity. Spoofing, multiple routing, and other antidetection measures further compound efforts by either law enforcement or national defense personnel to characterize their respective targets, even without the loss of time that may be required to determine whose jurisdiction the investigation of questionable activity involves. Guidance in this respect must come from top policy-makers, who must define a clear and singular vision of the direction and form such interagency collaborations should take. The creation of an empowered joint guidance and task-allocation structure would assist in avoiding waste of resources, duplicative expenditure of resources, and bureaucratic or sluggish response capabilities.

Finally, and perhaps most importantly, the two communities must continue their efforts and commitment to striking a balance between privacy and civil liberties on the one hand and security on the other. In doing so, both must overcome mistrust by the public—perhaps for different reasons but with no less impact—in establishing and expanding their roles and responsibilities with regard to receiving and handling information regarding private-sector incidents and safeguarding the borderless economy.

Areas of Potential Synergy

As already discussed here and elsewhere, the advent of emerging technologies and the borderless economy has tandem effects on both the economic and national security of our nation. In order to determine the feasibility and potential effectiveness of a collaborative effort between the law enforcement and national defense establishments, it is also necessary to identify areas of potential synergy. Some promising areas include:

Information sharing: Information regarding a singular incident or pattern of cyberthreats and/or vulnerabilities can be and is acquired by both communities.[2] Finding a methodology for sharing this information maximizes the accuracy potential of analyzing the import of such information, along with the ability to identify and address the nature of the cyberthreat or vulnerability. Particularly with regard to the speed with which a potentially catastrophic situation can develop, a seamless flow of information sharing is critical to facilitating early warning and detection systems: an essential component for any emergency response plan to be implemented.

Pooling of assets: Problems associated with a lack of personnel, resources, and funding are ever present in both communities. Pooling of such assets in areas of overlap and synergy will maximize efficiencies, provide greater depth and back-up capabilities, and provide some relief for both communities in the area of staff shortages and hiring freezes.

Different perspectives: Exchanging perspectives from both communities, as with any convergence of different viewpoints, will assist in leading to a broader scope of analysis and help identify both corroborative and conflicting theories and conclusions. A cooperative and honest dialogue from a variety of viewpoints will likewise maximize the potential for accurate analysis of information at hand.

EVOLVING FORWARD FROM THE EXISTING FOUNDATION

The National Infrastructure Protection Center

The formation of the National Infrastructure Protection Center (NIPC) in February of 1998 signified the federal government's commitment to addressing issues relating to critical infrastructure protection. Among other responsibilities, one of the key issues that fell under the NIPC's scope was exploring methods for providing law enforcement investigation and response capabilities. The NIPC has made progress in achieving its mission,[3] but the past three years have likewise allowed a sufficient period for assessment of how to address some deficiencies present in the current approach.[4] One area that requires more focus is that of

transitioning law enforcement from its traditional role into one more collaborative with the national defense community.

With regard to the law enforcement area, the NIPC serves as sector liaison for the Emergency Law Enforcement Services (ELES) sector at the behest of the FBI. The NIPC marks its progress to date in fulfilling this role by its delivery of the ELES Sector Plan on 2 March 2001. The NIPC also developed a "Guide for State & Local Law Enforcement Agencies" that is intended to aid state and local law enforcement agencies in protecting themselves from cyberthreats and attack. The NIPC has likewise made significant strides in creating interagency working and information sharing relationships, not the least of which includes the acquisition of detailees from various U.S. government agencies, many of whom hold senior leadership positions within the NIPC.[5]

The Road Ahead

1. Fully understanding the capability for integration of law enforcement and national defense objectives.

In formulating a national policy to address the issues raised by the borderless economy and critical infrastructure protection, the lead agencies for coordination (and possibly management) functions in effecting that policy are most likely to be embedded in the law enforcement and national defense communities.[6] Adopting this as a baseline assumption, there must be a comprehensive and realistic understanding of what the capabilities for (and limitations of) integration of the law enforcement and national defense communities are beyond what has already been accomplished. This requires an honest and critical assessment of the relationship—both potential and realized—between the law enforcement and national defense communities. As part of this examination, joint primary objectives and goals should be re-assessed and re-prioritized, taking into consideration the success and identified deficiencies of the past three years. Efforts that have achieved success or show progress should be fortified, and commitment and consolidation of available resources must be made. An adjusted, flexible milestone schedule should also be established setting forth reasonable time frames for achievement.

2. Integration of the third pillar: the private sector.

While significant efforts have been made with regard to creating a working relationship between the law enforcement and national defense establishments, a key issue that *must* be made a priority and dealt with is the integration of both communities with the private sector.[7] Unlike traditional law enforcement or national defense scenarios, critical infrastructure protection and the borderless

economy absolutely mandates full and equal cooperation and information sharing with the private sector. Achieving this relationship and accompanying information-sharing protocols in a manner that will maximize the chances for success is not a personnel or resource issue: it requires a sea change in cultural mindset. At a minimum, it requires either a resurgence or revamping of the approach taken to date.

As an example, over three years after the NIPC's establishment, and its assignment under Presidential Decision Directive (PDD) 63 as the entity responsible for overall coordination, fundamental issues with regard to achieving full collaboration with the private sector—a *key* requirement for success—remain unaddressed. The NIPC notes (and justifiably so) its recent focus on strengthening its InfraGard Initiative as a step in the right direction. All 56 FBI field offices have InfraGard chapters, and emphasis is appropriately placed on the importance of respecting the proprietary nature of much of the submitted information and granting confidentiality to private sector members with regard to self-performed sanitation of information provided to the Infragard network. Implementation of the InfraGard Initiative, however, clearly is not enough. Of the four information sharing and analysis centers (ISACs), NIPC has established an information-sharing partnership with only one—the electric power industry.[8]

The failure to establish the critical information-sharing collaborations can be pinpointed to two fundamental incompatibilities between law enforcement and the role assigned to it pursuant to the critical infrastructure efforts and PDD 63. private sector entities, driven largely by the faith of their investors and shareholders, are understandably reluctant to share information with competitors or to disseminate information that can damage their reputations and the public confidence placed in them as operating businesses. In addition, common sense dictates that such entities would be equally if not even more reluctant to share information with governmental agencies that have either regulatory authority over them or the power to prosecute the very industries with which they are seeking full cooperation. Cooperating in the manner being requested of them in today's legislative environment essentially equates to the private sector accepting, without protection, that the release of potentially negative information to the NIPC or one of the ISACs could easily lead to prosecution or more stringent regulation (and possibly sanctions) from the very agency which is supposed to be cooperating with the affected industry.[9]

ROADMAP FOR CONSIDERATION

Achieving a smooth and successful transition between law enforcement and national defense efforts in addressing the challenges and threats posed by the advent of the borderless economy requires: (a) a clearly defined national policy

that provides strong guidance to both communities in defining their roles and responsibilities; (b) mechanisms for continuing re-assessment; and (c) a multi-prong approach that can accommodate course corrections. Other items for consideration in addressing the transition between law enforcement and national defense include:

- Consideration as to whether the NIPC should somehow be segregated from the FBI. Separation would help solve some of the perception issues discussed above and likewise address some of the obstacles present currently hindering the private sector's integration with the ongoing governmental efforts, particularly in the area of information sharing. The NIPC could be re-established either as a stand-alone entity (still inter-agency staffed) or as a coherent but separate unit within a different agency (one more management-focused and oriented than the FBI, such as FEMA). Alternatively, a parallel entity or entities could be established outside of the FBI that would serve the same role as the NIPC has done for the government sector, but focusing on the private sector without having to struggle with the potential pitfalls created by the fundamental conflict between reconciling law enforcement mandates and the voluntary provision of private sector information.[10] In any event, the NIPC should do a hard assessment of its cultural mindset and develop a "fresh look" plan to lay out its intended strategy for achieving fundamentals of foundational critical infrastructure protection requirements and should:

  - focus on building/maintaining credibility with regard to safeguarding and disseminating private sector information.
  - focus on better collaboration with other governmental agencies.
  - consider emulating FEMA (which serves a role based more on serving in a coordination/management role than as "technical experts for all seasons").

- The need to shift the mindset of both communities, but especially law enforcement, from a reactive to a proactive paradigm. In the same way law enforcement has initiated programs focusing on community policing and outreach to lower crime rates and engage citizen involvement, so must the national effort restructure itself to incorporate analogous measures in order to establish the strongest firewalls against cyberthreats.

- The need to create stronger and better-defined partnerships between all relevant law enforcement, intelligence and national defense agencies (as well as other government agencies).[11] This effort should include re-examination and re-assessment of the structure(s) currently in place, and identification of resulting efficiencies and weaknesses. Consideration

should be given as to whether an overhaul is required to address deficiencies (both internal and external to involved agencies). Directional decision-making processes should be centralized, and consensus sought without the creation or encouragement of bureaucratic or sluggish response capabilities.

- Particularly when addressing a transformation of roles and responsibilities involving law enforcement, as well as the issues discussed above with regard to information-sharing relationships with the private sector, the need to re-examine legislation currently in place (and being proposed) to deal with borderless economy issues should clearly be priority. This analysis should consider a number of areas requiring legislative guidance, including but not limited to:[12]

  - Antitrust and competitive concerns
  - Corporate and D&O liability
  - FOIA exemptions for information voluntarily submitted

- The establishment and/or refinement of reasonable and acceptable parameters and clearly defined protocols for information sharing among/between all interested and relevant entities/parties. Achievement of working protocols requires all involved parties to overcome cultural mindsets and trust each other and, simultaneously, to behave in a manner to earn and retain the trust reposed in them.

- The need to engage in extensive public education and outreach. The potential impact on privacy and civil liberties concerns mandates educating the public and engaging in outreach initiatives.

- Finally, due to the nature of the technology as well as the extraterritorial aspects of dealing with the borderless economy and national security concerns, there is a need to continue engaging in international dialogue and partnerships.

CONCLUSION

Great progress has been achieved in creating a new paradigm for dealing with emerging technologies and the reliance of America's critical infrastructure upon those technologies. This includes steps taken by two of the communities that are arguably confronted by the most significant challenges posed by the ascendancy of the borderless economy: law enforcement and national defense. It is clear, however, that this is only the beginning and that more needs to be done. The challenges facing our nation demand a continuing commitment to achieving a

clear understanding and consensus on the parameters of lawful action that can be undertaken and the responsibilities of all affected entities, while still maintaining the delicate and often changing balance between national security and preservation of the civil liberties of our nation's citizens. This understanding must be formed not only as to the law enforcement and national defense communities, but also as to the private sector and ultimately to the American people.

This nation, beyond all others, stands to profit and benefit most from the borderless economy, and concurrently holds the greatest capability of taming the technology so that it cannot be used against our citizenry or national security interests. Accomplishing this, however, requires unification of commitment, effort and vision, along with a continuing dialogue that provides those tasked with our protection with the flexibility, innovation, and resources that are required to achieve the objectives desired.

Angeline G. Chen holds a J.D. from Villanova University School of Law and an LL.M in International and Comparative Law, with distinction*, from Georgetown University Law Center. She spent several years in private practice, where she specialized in complex litigation concentrating in the areas of antitrust and securities. Subsequently, she served as Assistant General Counsel for INTELSAT, an international organization that owns and operates a geosynchronous satellite system providing telecommunication services worldwide. In this position, her primary responsibilities included serving as principal legal advisor for all of INTELSAT's major programs procurements (satellites, TT&C, and launch services) and contracts, new business ventures, litigation, and investigatory matters (including congressional inquiries). In addition, Ms. Chen was responsible for creating and developing an export/import controls and compliance infrastructure within INTELSAT in preparation for the organization's privatization (which occurred in July of 2001).*

More recently, Ms. Chen served as the Deputy Associate General Counsel for Information Security at the National Security Agency (NSA). At the NSA, her primary areas of responsibility included telecommunications, space and commercial affairs, spectrum management, technology transfers, and critical infrastructure protection matters. In addition, she served as a liaison to interagency efforts relating to CFIUS matters.

Based on her background and expertise in high technology issues, Ms. Chen was invited to develop and team-teach a course in Cyberterrorism and National Security Law during the Spring 2001 semester at George Mason University Law School, along with former Secretary of the Army and Virginia Congressman John O. Marsh. This course, which focuses on legal and policy issues relating to critical infrastructure protection, has been integrated into George Mason's Technology Law program and will be offered again for both the Fall 2001 and Spring 2002 semesters.

Ms. Chen currently serves as Associate General Counsel and Director of Compliance and Policy at International Launch Services, an international joint venture established by Lockheed Martin and Krunichev-Energia to market several of the world's premier launch vehicle systems, including the American-built Atlas and the Russian-built Proton launch vehicles.

Notes:

1. The statements and opinions set forth herein solely reflect those of the author, and do not purport to represent the positions or opinions of any of her employers, past or present.
2. Indeed, existing linkages between cyber-oriented activity and other incidents can also be more easily identified.
3. *See, e.g.,* Statement of Ronald L. Dick, Director, NIPC, FBI, before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information (25 July 2001), located at http://www.senate.gov/~judiciary/te072501st-dick.htm.
4. *See* GAO Report, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities" (May 2001) (hereinafter "GAO Report").
5. NIPC's staff includes personnel tasked to the NIPC from: FBI, CIA, NSA, GSA, DOT/FAA, CIAO, Army, Office of the Secretary of Defense (Navy Rear Admiral), the Air Force Office of Special Investigations, Defense Criminal Investigative Service, and others. See Statement of R. Dick, *supra note* 1.
6. This assumption is based on a number of factors, not the least of which is that in most if not all cases, the activity at issue already falls within the jurisdiction of one or both communities, either as a permissible target or possible federal crime, but in either instance as an appropriate matter for further analysis and evaluation.
7. *See* Stevan D. Mitchell, *PCCIP to PDD: First Steps in Infrastructure Assurance* at page 8 (noting that a workable information sharing relationship requires trust and cooperation between public and private sectors).
8. *See* Statement of Robert F. Dacey, Director, GAO Information Security Issues, before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information (25 July 2001), located at http://www.senate.gov/~judiciary/te072501st-dacey.htm.
9. *See* Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, 7 Comm. Law Conspectus 153, 170 (Winter 1999).
10. *See* Mitchell, *supra note* 6, page 13 (proposing establishment of several structures to met public and private demand for more and better threat and vulnerability information: one housed at the FBI and other(s) "in the private sector for information that might not otherwise flow through traditional law enforcement channels.")
11. *See* GAO Report, *supra note* 3 (recommending that the NIPC formalize relationships with other federal entities and private sector ISACs).
12. It should be kept in mind that many existing laws and regulations cover illicit activities that are conducted over the Internet already. Any new legislation must be carefully drafted so as to avoid duplication of existing legislation and the creation of potentially conflicting regulations.

Use of the Defense Production Act of 1950 for Critical Infrastructure Protection [1]

By Lee M. Zeichner

THE DEFENSE PRODUCTION ACT AND CRITICAL INFRASTRUCTURE PROTECTION

As we move beyond the fifty-year anniversary of passage of the Defense Production Act of 1950 ("DPA"),[2] both Congress and the administration should revisit the genesis of this profound legislative framework.[3] Congress debated the DPA during a dynamic period in our national history. With the memory of Pearl Harbor fresh in the Congress' institutional psyche, and an undeclared conflict in Korea, both Congress and the administration cooperated to develop a legislative framework that integrated competing defense, national economic security, and related policy demands.

Overhaul of the DPA for Critical Infrastructure Protection

Close to five years after the President's Commission on Critical Infrastructure ("PCCIP") issued its report,[4] and now into the second presidential administration to govern in an information-based economy, the nation lacks an integrated legal, policy, and management philosophy to support critical infrastructure protection efforts.

Critical infrastructure service failures could result in significant catastrophic damage; in many cases, service failures could cascade into multiple other failures in ways that are not fully understood or predictable.

Multiple reports, technologists, and commentators have acknowledged the nation's significant reliance on critical infrastructure services. Our economic strength and stability are linked inextricably to reliable delivery of essential services—including information and communications, energy, financial, transportation, emergency medical and police, and water. Paradoxically, our robust capacity to deliver critical infrastructure services over information networks leaves the nation vulnerable in new and different ways. Economic security, long an element of national security and national defense, depends on the reliable delivery of these critical infrastructure services more than ever.

However, governance and policy solutions from the "physical world" do not operate seamlessly in cyberspace. Reliance on information systems and networks creates diverse risks—threats and vulnerabilities that are not addressed in traditional plans and processes. Problems and solutions cross over political boundaries and challenge many of the legislative frameworks and philosophies developed during the past 50 years.

As a result, managing infrastructure disruptions demands alternative preparedness, response, and restoration strategies.

Year 2000 Cyber-Solutions Dismantled

Critical infrastructure protection requires an integrated policy framework. Risk management, public-private collaboration, national defense, law enforcement, intelligence, emergency preparedness, and response—all are significant elements of an integrated solution. In order to prepare for the Year 2000 glitch, this nation was forced to piece together an integrated governance framework; the capabilities simply did not exist.[5]

Much of the important work conducted prior to the Millennium Rollover involved developing bridging mechanisms to cross over political boundaries and programs for the physical world. Unfortunately, both the federal government and state governments have for the most part dismantled solutions developed in preparation for the Year 2000 glitch, including physical watch centers as well as integrated policy frameworks. Consequently, there are considerable deficiencies in the nation's ability to prepare for, respond to, and recover from extensive critical infrastructure service failures.

DPA as a Component of an Integrated Framework

The DPA is one of the most significant congressional authorities for supporting critical infrastructure protection efforts. Since President Truman signed the DPA into law in 1950, successive administrations have stitched the DPA delegations into a safety net of Executive Orders, decision directives, and other significant legal doctrine—most of which implement our most vital defense and security programs.[6] A congressional and administration strategy that diminishes the full reach of the DPA undermines our ability to ensure essential operational responsibilities for the national security and defense.

This paper examines four issues in support of broadly applying the DPA to critical infrastructure protection activities:

1. Why did the Truman administration encourage Congress to pass the DPA and how does history inform the current debate?

2. What role does the DPA play as a legislative tool in addressing complex critical infrastructure challenges?

3. What are the competing legislative philosophies for managing critical infrastructure protection?

4. Why must Congress and the administration collectively develop an integrated framework that includes and promotes use of the DPA? What are the ramifications for the nation if the government fails to resolve these relevant policy challenges?

TRUMAN AND CLINTON: DEFENSE PRODUCTION ACT PHILOSOPHIES

Truman Introduces the DPA framework

Slightly over 50 years ago, during the summer of 1950, the Truman administration's Director of the National Security Resources Board entered the Dirksen Building with his counsel for the first of a three-day hearing on legislation entitled the Defense Production Act of 1950. The administration proposal combined certain emergency economic powers exercised during and after World War II into a permanent legislative framework.[7] These powers were necessary to place goods and services where they were most needed.

President Truman could exercise these powers during peacetime and absent any declaration of national emergency.

The core of the proposal would allow the president to prioritize and expedite delivery (or allocation) of critical materials. If company A contracts to deliver widgets to company B, but the government needs the widgets—whether for itself or for Company C, the president could so order the prioritization of contract delivery according to terms "necessary to promote the national defense."

For three days, members of the Banking and Currency Committee debated a series of questions exploring the relationship between economic stability, national defense, and the projection of power and national authority. The senators' questions revealed deep concerns over both the Cold War and an ongoing need to restructure national economic programs, courses of action, and priorities:

- Does economic and industrial stability translate into the projection of power and, if so, how does this promote the national defense?

- How much extraordinary authority should the Congress delegate to the president during peacetime? That is, do we need a legislative framework if there is no war, significant military conflict, or presidential declaration of emergency: Indeed,

- Could Congress trust the president to administer the legislative framework? If not, how could Congress possibly perform these responsibilities?

The exceptional debate that followed raised complex questions for a nation that had learned more than a little about national defense during the preceding decade. The irony of delegating extraordinary economic powers to preserve a free economy was not lost on the Senate that week; but the complexity of mobilizing after Pearl Harbor—not to mention the perception of the country as weak and vulnerable, which might have precipitated the attack—was fresh on the mind of each and every senator. The debate conveyed a profound sense of national import where reasonable public servants could differ.

Members of the Banking and Currency Committee also understood that the nation was entering the Cold War and by week's end sided with the Truman administration. There was no solid agreement on how the new world order impacted national defense, but the Senate clearly understood the importance of bridging complex and emerging policy concerns into a single, integrated legislative framework.

Clinton Administration debates use of DPA for Y2K crisis

A half-century later, as the nation prepared for the Year 2000 ("Year 2000" or "Y2K") glitch in the summer of 1999, senior officials in the Clinton administration and their counsel met to discuss whether the DPA could and should be used in the event a Y2K infrastructure outage resulted in a national crisis. Senior leaders grappled with two questions: What is the national philosophy for preparing for, responding to, and recovering from significant critical infrastructure outages, and could the DPA be used to expedite delivery, or allocation, of goods and services to fulfill these goals?

Multiple areas of disagreement emerged in the six-month Y2K discussions. The most significant concerned the relevance of the Federal Response Plan framework in managing critical infrastructure disruptions of national significance and negotiating the roles and responsibilities of multiple agencies in managing a national cyber-crisis.[8] Pursuant to Executive Order 12919, signed in 1994, FEMA is charged with coordinating plans and programs among the civilian agencies for national defense industrial resource preparedness issues.[9]

But, did it make sense in the Information Age to saddle FEMA with responsibility for both cyber and traditional natural disaster management? In addition, what was the best process for negotiating and coming to agreement on priorities? If a significant cyber-disruption occurred, how would the consequences be managed and prioritized? Should the federal government seek to restore services as quickly as possible via the DPA or manage the consequences of the disruption through traditional means, such as via the Federal Response Plan?[10] How would law enforcement, intelligence, and defense issues be parsed by FEMA within the framework developed by the Clinton administration?

The lack of any pertinent congressional testimony, debate, or other legal guidance on use of the DPA unquestionably impaired the administration's ability to settle these disagreements.[11] Senior administration officials debated the issue late into December 1999. As the Millennium Rollover came and went, no final agreement was ever reached.[12]

Answers to these questions have significant impact on whether to use the DPA, and if so how broadly to interpret its terms. In sum: As we enter the 21st century, how does "national defense" relate to the delivery of critical infrastructure services? Specifically:

- What is the relationship between national defense and the orderly functioning of the nation's critical infrastructure services?

- If the DPA could be used, what prioritization plans and policies were in place to determine during a crisis which entities benefitted from the expedited delivery of goods and services?

- Did the nation understand interdependencies among infrastructure systems? Was restoration of one type of infrastructure (e.g., electricity) more important than another (e.g., communications)?

From Truman to Clinton: Common Themes

In many ways, the Clinton administration's debate over use of the DPA for Y2K failures echoes the Truman administration's dialogue with the Senate Banking and Currency Committee. As in the 1950 debate, both camps agreed that the landscape had changed—whether the emergence of the Cold War or the advent of the Information Age. However, two camps emerged reflecting significant philosophical splits within the national security and emergency management communities.

The first camp cited the DPA language, and legislative intent, to demonstrate that Congress had never meant to apply the DPA to information age issues. Absent "scuds and missiles" or a declared national emergency, use of the DPA was both inappropriate and unnecessary. The second camp argued that the DPA might be necessary to prioritize goods and services for fixing and restoring critical infrastructure systems that had failed because of he Y2K bug. This use, they concluded, fulfills the DPA's legislative intent in maintaining a strong industrial and military base.

WHAT IS THE NATION'S PHILOSOPHY FOR MANAGING CRITICAL INFRASTRUCTURE RISK?

This section discusses the need for an integrated governance philosophy for managing critical infrastructure disruptions of national significance. This philosophy is more important than ever, given the lack of congressional and administration agreement on programs and processes to manage critical infrastructure failures at this time. Within the federal government, administration of the Year 2000 glitch revealed multiple "competing" philosophies. In hindsight, the national Y2K effort was highly successful.[13] Throughout the preparation process, however, it was obvious that the nation was not prepared to respond to and recover from a national critical infrastructure failure.

In an effort to define policy and management objectives for critical infrastructure failures, this section examines five legislative models and philosophies: (1) Integrated Risk Management (PDD-63) model, (2) Traditional Emergency Preparedness, (3) Law Enforcement and Intelligence, (4) National Defense, and (5) Consumer Protection.

Beyond PDD-63: An Integrated National Risk Management Philosophy

Only through an integrated risk management governance philosophy can the nation develop appropriate programs for protecting the nation's critical infrastructures. A legislative program should support and further this philosophy.

Since release of Presidential Decision Directive-63 ("PDD-63") in May 1998, the United States has embarked on an aggressive critical infrastructure program. More than any other country, the United States has developed a progressive philosophy for critical infrastructure policy coordination, development, and analysis. Significant themes include:

- At the core of critical infrastructure protection is a concern for national security.

Since its inception in the aftermath of the tragic Oklahoma City bombing, critical infrastructure protection has always focused on widespread and catastrophic damage. In most cases where infrastructures fail—for whatever reason—owners and operators in industry and government are typically able to manage response and recovery efforts through normal business and risk management processes. For purposes of the Defense Production Act analysis, this is a significant distinction. Congress never intended the DPA to be used for general business purposes or for emergencies that could be managed under normal business continuity and disaster preparedness programs. However, conversely, where such damages could result, use of the DPA, as part of an integrated framework, is both prudent and appropriate.

- Critical infrastructure service failures could result in significant catastrophic damage; in many cases, service failures could cascade into multiple other failures in ways that are not fully understood or predictable.

A second characteristic of critical infrastructures is their interdependency with other critical infrastructure systems and services.[14] The prudent use of the DPA to prevent catastrophic downstream or cascading damages must be considered. Often a failure to restore service will lead to other infrastructure failures. Adopting alternative consequence management philosophies under these circumstances, which includes use of the DPA, is vital.

- Critical infrastructure protection is a shared responsibility.

Critical infrastructure protection involves unique partnerships. Not all partnership activities between the public and private sectors support the specialized needs of the critical infrastructure community. Critical infrastructures are largely owned and operated by industry and state and local governments. In many cases, the research and development that lead to infrastructure advancements is conducted within particular portions of the academic community. Concerns are highly operational, focusing heavily on service delivery.

In contrast, many of the programs established for traditional emergency response purposes focus on first responder capabilities and needs. Emergency medical, police, and fire rescue often have dramatically different goals and skills. This is not to say that these divergent communities do not need to be aligned—in fact, they do.[15] It makes little sense, however, to assume that preparedness and response activities in one community will provide similar value in all others.

- Successful critical infrastructure protection leads to economic stability and a more enhanced national defense.

The final core attribute of a critical infrastructure policy is that full operational capability—an integrated national critical infrastructure program with improvements in reliability of service—projects national authority and power, economic stability, and ultimately promotes the national defense. Use of the DPA as part of an integrated philosophy furthers these goals, which are at the core of the DPA's purpose.

For purposes of Defense Department functions and operational needs, this should be fairly obvious. The Defense Department relies heavily on infrastructure services, whether conducting operations at home or abroad. A failure to develop reliable service delivery patterns would have catastrophic effects on our ability to project power overseas.

Traditional Emergency Preparedness

The repeal of the Civil Defense Act of 1950 by the Stafford Act almost 10 years ago set the parameters of the current emergency preparedness and response legal and policy framework. Pursuant to the Stafford Act, and the Federal Response Plan that implements operational responsibility under that law, our nation relies heavily on traditional emergency preparedness programs and policies to manage a range of complex disasters.

As the Year 2000 crisis demonstrated, our nation lacks a similar preparedness, response, and restoration framework specifically constructed to include critical infrastructure protection. Many commentators have suggested applying traditional emergency preparedness processes to critical infrastructure protection. This is principally how the nation managed preparedness for the Year 2000 transition. However, the Stafford Act, and the programs that are implemented under the legislative framework, were never intended or designed for critical infrastructure protection.[16]

There are several important distinctions. First, the underlying philosophy for most emergency preparedness policies and programs is to mitigate the damages of a crisis. This framework, which is both successful and well integrated through years of trial and error, does not traditionally include industry critical infrastructure disruptions—a private sector concern. This is so even where the disruptions adversely impact the delivery of critical federal government services. As discussed elsewhere, the Y2K Operations Supplement to the Federal Response Plan *explicitly excluded* core critical infrastructure activities.[17]

Second, the funding mechanisms for providing federal assistance and aid are set in law. Stafford Act funding for emergency response activity flows from the federal government under conditions set by the Stafford Act and its administrative

guidance. For example, during Y2K, a presidential "emergency" was needed—as opposed to a "major disaster" declaration.[18]

Third, the amount of aid needed to support critical infrastructure disruptions is unknown. federal government administrators understand the cost of traditional emergency preparedness activities. The cost of critical infrastructure disruptions is not well understood or easily quantifiable. Cyber-related disasters could result in enormous damages absent appropriate mitigation programs and processes. Finally, traditional emergency preparedness goals are accomplished in today's legislative framework by aligning federal disaster relief programs with similar operational structures across the federal government and at the state and local levels. Long-term partnerships and relationships—which are crucial for disaster management capability, are built on skill sets, goals, and arrangements vastly different than those in the critical infrastructure community.

Law Enforcement/Intelligence

Similar to traditional emergency preparedness, a pure law enforcement or intelligence philosophy will not, *by itself*, resolve complex critical infrastructure challenges. Historically, the nation moved in that direction shortly after the Oklahoma City bombing with release of PDD-39. Two years later, the federal government imported PDD-39 into the Federal Response Plan mechanism as the Terrorism Annex.[19] This policy distinguished between consequence management and crisis management—creating room in the aftermath of an incident for law enforcement to investigate and fulfill its congressional responsibilities.[20] Where the attack is ongoing, law enforcement and intelligence gathering are crucial to locating and stopping the damage. Room for consequence management authorities to conduct their work is negotiated pursuant to the Federal Response Plan mechanism.

How would a law enforcement philosophy and framework support and fulfill critical infrastructure objectives? In many cases, policy choices may exist in opposition. As in the Year 2000 preparations, it is unclear whether significant infrastructure outages result from a malicious nation-state attack, teenage hacker, insider mistake, or some other source. Irrespective of the source of the outage, each of the policy choices is valid. The challenge, as argued, is integrating them into a cohesive framework that reflects the nation's best interests.

National Defense

How would a national defense philosophy align with critical infrastructure goals? Since 1995, multiple commentators have encouraged a national defense approach

to resolving critical infrastructure protection. These opinions include: (1) Require the Defense Department institutionally to manage and coordinate a national critical infrastructure program; (2) Require the Defense Department to undertake executive agency responsibility for a coordinated incident response and restoration center; or (3) Wrap critical infrastructure protection policies under the rubric of Homeland Defense or Homeland Security.

At a minimum, the Defense Department is a customer of critical infrastructure services and must be able to negotiate a level of performance consistent with its goals. Similar to the other issues above, identifying a critical infrastructure framework will lead to appropriate analysis of how the Defense establishment will align with other stakeholders and constituencies.

Consumer Protection

The final philosophic and legislative option for managing critical infrastructure is consumer protection. A consumer protection methodology provides, at a minimum, assistance and information to support consumer goals and options. Consumer protection was a critical component of the significant work performed by the President's Council on Year 2000 Conversion. One of the valuable lessons from Y2K is the importance of managing consumer confidence, providing information to assist consumer decision making, and supporting awareness as a part of any national effort. However, consumer protection issues do not rise to the national defense level that the DPA demands.

Summary—Philosophic Link to DPA

At the core of critical infrastructure protection philosophy is a concern for national security, national defense, and the public health and welfare. Critical infrastructure defines a set of policy priorities—i.e., managing competing policy concerns and, where necessary, prioritizing infrastructure service delivery over other equally plausible policy choices.

The Defense Production Act is the principal legislative tool for managing critical infrastructure operational needs. Were the nation to require critical infrastructure service delivery, then the full and robust use of the DPA would be essential. Critical infrastructure preparedness, response, and restoration could all benefit from using the DPA in a judicious and targeted manner.

THE ORIGIN AND MISPERCEPTIONS OF THE DPA

The debate over application of the DPA for critical infrastructure is ultimately a valid disagreement on how the nation should prepare for, respond to, and recover

from critical infrastructure incidents of national significance. The DPA must be one of the tools available to the administration to manage complex critical infrastructure disruptions.

That said, there is limited agreement on whether and to what extent the DPA could be used for those purposes. Some of these disagreements are factual—such as, whether critical infrastructure incidents truly rise to the level of national import and significance. Other disagreements are more philosophic, such as whether the nation needs an alternative "preparedness and response" framework to manage critical infrastructure protection. Finally, some disagreements are technical and legal. These include tracing back the legislative intent of Congress in creating the DPA and applying significant terms such as "national defense" to information age challenges.

This section argues in favor of using the DPA as part of a larger critical infrastructure legislative program. The reasoning and assumptions articulated include:

- Critical infrastructure incidents can result in significant national damage.
- The federal government relies heavily on the reliable supply of critical infrastructure services for serving national defense needs.
- The government must consistently project strength, economic stability, and political cohesion. Reliable delivery of critical infrastructure services is a cornerstone of these goals.

There are multiple misperceptions about the DPA, many of which were debated during its introduction in 1950. In 1975, 25 years after introducing the DPA, the Congress' Joint Committee on Defense Production again thoroughly examined the DPA as well as the overarching framework in which the DPA had been used.[21] From these and other discussions, there is a rich library of original history from which current decisions might be measured.

What is "National Defense"?

The most important legal trigger for use of the DPA is the meaning of the term "national defense." To take advantage of the programs in the DPA, the president must find that a "national defense" nexus exists. Thus, in the context of critical infrastructure disruptions, the president must make a determination that the expedited delivery of goods or services are "necessary to promote the national defense." From the first day that President Truman proposed the DPA, through Y2K and the recent use of the law by the Bush administration,[22] no single topic has garnered more debate and disagreement than the meaning of this term.

Since 1950, Congress has adopted two definitions. The first, also known as the traditional definition, includes those "programs for military and energy production or construction, military assistance to any foreign nation, stockpiling, space, and any directly related activity."[23] The second, added in 1995, links use of the DPA to the Stafford Act; expanding the term to include "emergency preparedness activities conducted pursuant to title VI of the [Stafford Act]."[24]

Congress' decision to extend the term "national defense" to include "emergency preparedness activities conducted pursuant to the [Stafford Act]" has engendered development of two alternative positions. Some have taken the position that the amendment only grants presidential authority to engage in certain activities that the director of FEMA is authorized to engage in, as enumerated in Title VI of the Stafford Act. Others, looking to Title VI in its entirety, adopt a more-expansive view, arguing that "emergency preparedness" is defined broadly in Title VI, and that it includes, but is by no means limited to, those activities specified in Title VI.

Misperceptions

Debates over the meaning of national defense during the Y2K discussions suffered from lack of tangible legislative history and context. As a result, multiple misperceptions inappropriately drive policy and decision-making.

The first significant misperception is that the president may activate the DPA solely for war or mobilizing to go to war. As the discussion on national defense demonstrates, the president must, at a minimum, make a national defense determination. However, Congress has never limited the application to wartime necessity. In fact, many of the senators during the initial debates in 1950 queried the Truman administration on this point. The importance of developing an integrated approach to economic security, defense production, and national defense convinced the Senate that such restrictions were not in the best interests of the nation. To date, the DPA makes available materials, services, and facilities in both peacetime and during crisis.

For critical infrastructure purposes, this is an especially important aspect of the DPA. In most cases, critical infrastructure outages will not result from war or an act of war, although this is certainly possible. Rather, the DPA provides a far more practical framework for managing infrastructure outages far short of all-out war.

The second misperception is that the DPA is limited only to preparedness activities. The DPA provides the president with broad authority to expedite delivery of goods and services. Priority contracting and allocation powers, for

example, may be used in response and restoration as well as preparedness activities. In many ways, the DPA provides a type of insurance program, which can be used when needed. For response and restoration of critical infrastructure, the use of the DPA is essential. There are no similar congressional authorities that provide a framework for managing restoration and recovery efforts through expedited delivery of essential goods and services.

The third misperception is that the DPA may only be used after Congress or the president declares a national emergency; this, too, is false. For many senators involved in the original debates, this was the most troubling component of the Truman legislative proposal. Why should Congress delegate to the president broad peacetime and wartime authority based only on a national defense determination? However, ever since the 1950 debates, Congress has not required a national emergency determination as a trigger for use of the DPA.

For critical infrastructure purposes, the ability to activate the DPA absent a formal national emergency finding is practical and useful. Many critical infrastructure outages could lead to national emergencies, and this is part of the attraction for using the DPA. Having to first declare a national emergency would impinge on use of this significant authority.

CONCLUSION

This paper argues for Congress and the administration to examine an integrated legislative and policy framework to manage significant critical infrastructure disruptions. There is no framework in place that integrates multiple policies, such as traditional emergency preparedness, law enforcement, national defense, and risk management programs that prioritize restoration of infrastructure services.

The DPA is an important tool for use in managing critical infrastructure disruptions of national significance. A failure to apply the DPA to critical infrastructures leaves this nation unprotected from a cyberattack or significant critical infrastructure disruption. Critical infrastructure supports the national defense in multiple ways. Absent use of the DPA, Congress should begin work immediately on developing alternative legislative frameworks for managing national critical infrastructure disruptions.

Lee M. Zeichner is president of LegalNet Works Incorporated. LegalNet consults both industry and government on the development of information security law and regulation. Mr. Zeichner was senior counsel to the President's Commission on Critical Infrastruc-

ture Protection (1996-1997) and has been a consultant to the Critical Infrastructure Assurance Office since May 1998. Mr. Zeichner also served as legal counsel to the Y2K National Information Coordination Center. Mr. Zeichner is a graduate of Georgetown University Law Center (1988 cum laude). He graduated from the University of Florida (B.A. 1983, Phi Beta Kappa) and received his Masters from Stanford University. Mr. Zeichner is a member of multiple bar associations, including the Florida and DC Bars, the Court of International Trade, and the Court of Appeals for the Federal Circuit. Mr. Zeichner recently wrote Cyber Security & Corporate Liability, a guide for corporate counsel on information security and risk management laws and policies, published by the Lexis Publications.

Notes:

1. © Lee M. Zeichner, All Rights Reserved (2001). I would like to extend my deep appreciation to the National Archives Administration ('NARA") for their support in providing access to original Defense Production Act debates and related resource materials. NARA is a national asset. I would also like to thank my legal assistants, Morgan Allen, Alexis Ovitt, and Jeanne Geers for their superb research skills and capabilities. Finally, my gratitude to John McCarthy (USCG-ret) for his valuable insights in analyzing the activities surrounding Year 2000 policy discussions.
2. Defense Production Act of 1950, as amended, 50 USC App. § 2061 *et seq.* ("DPA"). This paper focuses exclusively on Title I authority to expedite the priority delivery of goods and services for the federal government's critical infrastructure goals and purposes.
3. For an excellent overview and analysis of the DPA, please refer to *Defense Production Act: Purpose and Scope*, by David E. Lockwood, Congressional Research Service Order Code RS20587 (Updated June 22, 2001).
4. The PCCIP recommended use of the DPA for national critical infrastructure disruptions. *See Protecting American's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection* at 81 (October 1997).
5. *See Amendment to Executive Order 13073, Year 2000 Conversion*, Executive Order 13127 (June 14, 1999).
6. *See*, e.g., *Assignment of National Security Emergency Preparedness Telecommunications Functions*, Executive Order 12472 (1984) (Restoring wireline communications for the federal government).
7. *See* U.S. Senate. Committee on Banking and Currency Congress of the United States. Defense Production Act of 1950 (to accompany by S. 3936), 81st Congress, 2d Session. (S. Rpt. 81-2250) 1950 at 45.
8. The Federal Response Plan is based on the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 USC § 5121 *et seq.* ("Stafford Act").
9. *National Defense Industrial Resources Preparedness*, Executive Order 12919 (June 7, 1994) (One exception relates to energy issues, which are coordinated by the Department of Energy).
10. As an example, a Federal Response Plan approach ruled out use of other highly responsive and successful programs that service critical infrastructure emergencies. *See*, e.g., Defense Priorities & Allocations System ("DPAS") (Highly flexible process for administering critical infrastructure crisis; DPAS is administered by the Office of Strategic Industries and Economic Security, Bureau of Export Administration (Dept. of Commerce) pursuant to the DPA. See 15 CRF Part 700).
11. Congress has not addressed the basic terms and definitions in the DPA for application in an economy that relies on critical infrastructure services. How, for example, do the terms

incorporate the nation's dependence on information services? "Energy" is clearly included in the DPA, but how does the energy infrastructure reliance on communications alter the statutory definition? See DPA definitions at 50 US App. § 2152.

12. This was not the first time senior officials within the Clinton administration carefully examined the DPA and its implementing programs. *See*, e.g., *Report of the Interagency Sub working Group of the national Security Council's Ad Hoc Interagency Working Group on National Security Emergency Resources Preparedness* (December 1996) (Administration working group recommends overhaul of Executive Order 12919, and other authorities, which implement the DPA).
13. The nation—including the state and local governments and industry—deserve high praise for resolving a potential crisis. But efforts to address lessons learned and to benefit from the experience have been lost. As soon as the Millennium Rollover passed, the Federal government dismantled valuable facilities, partnerships, and institutions, all of which offered significant value; similarly, in many state and local governments, valuable facilities and institutions were set aside.
14. For an excellent background on this issue, refer to *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office at Chapter 3 (July 1998).
15. There is, of course significant overlap. For example, first responders are increasingly under pressure to develop interoperable, more robust, and secure communications. Bandwidth and spectrum problems will increasingly plague first responder capabilities—both are critical infrastructure concerns.
16. The Stafford Act repealed the Civil Defense Act of 1950, which centralized emergency response process in the Executive Office of the President. 42 USC § 5121 *et seq*.
17. These included: (1) Business continuity and contingency planning necessary to ensure that vital services are not disrupted due to Y2K problems, (2) Reconstitution of Y2K-affected State and local information technology systems, (3) Cyberterrorist attacks (addressed in PDD-63), and (4) National security telecommunications emergencies in industry and in the Federal government *Y2K Operations Supplement to the Federal Response Plan* at 8 (1999).
18. For an excellent primer on programmatic particulars, refer to *Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures*, Report of the Subcommittee on VA, HUD, and Independent Agencies, Committee on Appropriations, U.S. Senate, GAO-01-837 (August 2001).
19. Terrorism Incident Annex to the Federal Response Plan. ("PDD-39 directs the undersigned departments and agencies to perform specific responsibilities that may affect the performance of their responsibilities under the FRP.")
20. Similarly, PDD-63 requires the National Infrastructure Protection Center to "monitor" reconstitution activities. Where owner/operators are unable to stop an attack in order to restore service, assistance from law enforcement and intelligence operations would be extremely valuable.
21. *See*, e.g., Hearings Before the Joint Committee on Defense Production, Congress of the United States, 94th Congress, 2nd Session (April 28, 1976).
22. See Memorandum for the Secretary of Energy, Electric Supply Shortage in California (January 19, 2001).
23. DPA, 50 USC App. § 2061, 2152(13).
24. 50 USC App. § 2152(13). Emphasis added.

National Security: The Definitions Landscape

By Jack Oslund

How is national security defined today? What are the United States' national interests? And where does critical infrastructure protection fit in?

Social, economic and environmental problems are worsening in many parts of the world. And diffuse and asymmetrical nuclear, biological, chemical, cyber and terrorist threats are emerging at the same time that distinctions between what is domestic and what is foreign are blurring.

This paper, written from a policy perspective, seeks to address these questions in the following manner. First, the conceptual evolution of national security and national interest, as debated by policymakers, strategists, and scholars, is summarized to provide a theoretical perspective. Second, reports by four recent high level commissions, comprised of former senior government and industry leaders, are analyzed to provide an operational perspective in terms of how they developed working definitions of these concepts and applied them to "the real world"—The Commission on America's National Interests,[1] The United States Commission on National Security/21st Century,[2] The Commission to Assess United States National Security Space Management and Organization,[3] and The President's Commission on Critical Infrastructure Protection.[4] Third, the inclusion of Critical Infrastructure Protection ("CIP") within the context of defining national security and national interest is reviewed. Lastly, recognizing that a national dialogue to revisit and redefine our understanding of national security and national interests is about to begin, a framework for the dialogue is proposed.

The need to redefine national security is not a new phenomenon. Each significant change in the geopolitical environment has brought with it a call for redefinition. Examples include the immediate post-Vietnam War era[5] and the immediate post-Cold War era.[6] This present era of globalization is no different with its significant set of new opportunities and challenges. National and international infrastructures and economies are becoming more interdependent and interlinked by increasingly efficient and converging, but vulnerable, telecommunications and computer systems. International economic competitiveness is requiring government policymakers to adapt new economic policies and industry leaders to restructure and consolidate. Social, economic and environmental problems are worsening in many parts of the world. And diffuse and asymmetrical nuclear,

biological, chemical, cyber, and terrorist threats are emerging at the same time that distinctions between what is domestic and what is foreign are blurring.

EVOLUTION OF THE CONCEPTS OF NATIONAL SECURITY AND NATIONAL INTEREST

Debates to define national security and national interest have been going on between and among policymakers, strategists, and scholars since the mid-1950s. There is no universal agreement on even theoretical definitions of these concepts

National Security

The earliest formulation of the concept of national security is attributed to Walter Lippmann who wrote in 1942: "A nation is secure to the extent to which it is not in danger of having to sacrifice core values, if it wishes to avoid war, and is able, if challenged, to maintain them in victory in such a war."[7] Within a decade after this formulation, and concurrent with the beginning of the Cold War, national security became the focus of foreign policy analysts. In his classic 1952 essay, Arnold Wolfers described it as "an ambiguous symbol."[8] Indeed, when the National Security Act had been enacted five years earlier to create an organizational framework for the federal government to integrate domestic, foreign, and military policies related to national security, it was notably silent with respect to what national security meant.[9]

While discussion of national security during and through the Cold War era was conducted primarily in terms of national defense and foreign policy, international economics was added to the national security agenda in the 1970s.[10] Subsequently, some strategic analysts "inappropriately argued that economic security [had become] the only crucial security dimension."[11] In the late 1980s with the demise of the Soviet empire and the Soviet state, proposals were made to expand the agenda to include natural resources, the environment, demographics,[12] human rights, drug traffic, epidemics, crime, and social injustice.[13] Responding to these proposals, Theodore Sorensen, former Special Counsel to President Kennedy, said that a narrow, not broad, definition of national security is required, and suggested that it could be achieved by building a bipartisan consensus around a very limited number of basic national security goals, while leaving room for partisan disagreement on their implementation.[14]

Despite the lack of an agreed definition, "national security" has been—and is being—applied in a number of public policy venues. Examples of its often complex and controversial application include: the continuing congressional debate to amend the Export Administration Act of 1979 that is intended to control the transfer of rapidly changing technologies in a dynamic international environ-

ment; the question of whether the electronic surveillance techniques that the law enforcement agencies employ should be publicly disclosed; and the 1998 Exon-Florio Amendment to the Defense Production Act of 1950 that is intended to address foreign takeovers of strategic U.S. high tech industrial firms. The most publicized application was the government's unsuccessful efforts to block the publication of the then-classified Pentagon Papers in 1971 that involved weighing national security concerns against the freedom of the press.

National Interest

Wolfers'1952 article on national security also identified national interest as a related vague concept that sought to explain a nation's behavior in terms of its perception of its national interest at a particular point in time.[15] When his essay was published, the debate on what constitutes the national interest was becoming polarized between the realists and the moralists (later called idealists). Over the years, opponents have criticized national interest-based foreign policy in terms of the complexity of defining the means and the ends of such a policy, of the problem of aggregating special interests into a national interest, and of whether it is retroactively read into public policies in which it may have played a marginal role or no role at all.[16]

Hans Morgenthau, an early and influential advocate of the realist school, argued that the point of departure of the foreign policy of any country should be the concept of national interest as defined in terms of power.[17] Through the years, Morgenthau's power-based formulation of the national interest has been challenged, but it has not been effectively refuted. Indeed, a year before she was named as the National Security Adviser in the present Bush administration, Condoleezza Rice strongly argued that American foreign policy in a Republican administration should refocus the United States on the national interest and the pursuit of key priorities. Further, "Power matters, both the exercise of power by the United States and the ability of others to exercise it."[18]

Interestingly, a comprehensive study of definitions of national interest in the 1890s, 1930s, and 1980s concluded that "there is no single national interest"[19] and, in so doing, reaffirmed the frequently expressed view that because the national interest of a nation is to satisfy its national needs, there are as many national interests as there are national needs.[20]

This concept, predictably, has been used as the basis for policy actions as national needs have arisen ranging from committing U.S. forces on foreign soil, to imposing or lifting trade embargoes, to allowing United States commercial satellite companies to compete internationally with INTELSAT when it was still an international satellite organization.

THREE COMMISSIONS OPERATIONALIZE NATIONAL INTEREST AND NATIONAL SECURITY

Three of the four previously mentioned Commissions were established on a bi-partisan basis to assess the role of the United States in light of the dramatic shifts in the world's economy and in its asymmetrical power structure—The Commission on America's National Interests ("Commission on National Interests"), The United States Commission on National Security/21st Century ("Commission on National Security"), and The Commission to Assess United States National Security Space Management and Organization ("Commission on Space Management"). The Commissions developed and applied working definitions of national interest and national security, based on the view that national security must find its anchor in U.S. national interests.[21] During the same period of time, the Executive Branch launched its CIP initiative.

Commission on National Interests

Privately organized and funded, the Commission was established in the mid-1990s to focus national debate on prioritizing the multiple U.S. national interests. The message of its July 1996 report was clear: Only a national interest-based foreign policy will provide priorities for American engagement in the world, and only a foreign policy grounded in American national interests will allow America's leaders to gain the support of the citizenry.[22] Further, a four-level hierarchy was proposed to clarify the numerous national interests based on the U.S. government being able "to safeguard and enhance the well-being of Americans in a free and secure nation": vital interests ("conditions that are strictly necessary. . . "); extremely important interests ("conditions that, if compromised, would severely prejudice but not strictly imperil the [government's] ability. . . "); just important interests ("conditions that, if compromised, would have major negative consequences for the [government's] ability . . . "), and less important or secondary interests ("conditions that are intrinsically desirable but have no major effect on the [government's] ability. . . ").[23]

Preventing the "catastrophic collapse" of major global systems (e.g., trade, financial markets, and supplies of energy) was listed as a first level "vital interest." Because these systems are dependent upon telecommunications and computer systems, CIP was implicitly placed at the same "vital interest" level as: the prevention, deterrence, and reduction of the threat of nuclear, biological, and chemical weapons attacks on the U.S.; the prevention of the emergence of a hostile major power on U.S. borders or in control of the sea; the prevention of the emergence of a hostile hegemony in Europe or Asia, and the insured survival of U.S. allies.[24] However, when the Commission addressed national interests in terms of "functional areas," CIP appeared at two levels. It remained as a first level

"vital interest" in the area of "International Trade and Investment" to the extent that it supports the prevention of the collapse of the international trade and financial systems.[25] In the functional area of "Terrorism, Transnational Crime, and Drugs," CIP's role in reducing the vulnerability of U.S. informational, financial, and military infrastructures to large-scale "cyberterrorism" was a second level "extremely important" interest.[26] CIP, in the functional area of "Cyberspace and Information Technology," also was related to "extremely important" interests in maintaining U.S. leadership in the development and application of information technology in the economic arena, and in embedding in the nation's technology and culture a greater awareness of the new vulnerabilities attendant in increased reliance on information systems.[27]

Commission on National Security

In mid-1998, this bipartisan Commission was chartered by the secretary of defense to conduct a thorough study of national security processes and structure. Based on a background futuristic study, a number of general conclusions were reached in the initial report in 1999, including: "rapid advances in information and biotechnologies will create new vulnerabilities for U.S. security" and "space will become a critical and competitive military environment."[28]

The second report, issued the following year, addressed national security strategy—a strategy "composed" of a balance between reaping the benefits of a more integrated world in order to expand freedom, security and prosperity for Americans and for others, and dampening the forces of global instability so that those benefits can endure.[29] Six precepts were presented as a guide to the formulation of the national strategy, although only the first precept was related directly to this paper and stated, "Strategy and policy must be grounded in the national interest. The national interest has many strands—political, economic, security, and humanitarian. National interests are nevertheless the most durable basis for assuring policy consistency."[30]

A hierarchy of national interests was developed, similar to the hierarchy that had been proposed by the earlier Commission on National Interests. However, three, rather than four, levels were proposed: "survival interests, without which America would cease to exist as we know it; critical interests, which are causally one step removed from survival interests; and significant interests, which importantly affect the global environment in which the United States must act. There are, of course, other national interests. . . . "[31]

"Survival interests" were America's safety from direct attack, especially involving weapons of mass destruction, by either states or terrorists, and the preservation of America's constitutional order and of those core strengths—educational,

industrial, scientific-technological—that underlie the nation's political, economic, and military position in the world.[32] CIP was considered among the "critical interests" at the next highest level: "Critical U.S. national interests include the continuity and security of those key international systems—energy, economic, communications, transportation, and public health (including food and water supplies)—on which the lives and well-being of Americans have come to depend. It is a critical national interest of the United States that no hostile power establish itself on U.S. borders, or in control of critical land, air, and sea lines of communications, or—in today's new world—in control of access to outer space or cyberspace. . . . "[33]

Commission on Space Management

Established pursuant to the FY 2000 National Defense Authorization Act, this bipartisan Commission held its first meeting in May 2000, less than a month after the release of the Commission on National Security's second report in which access to outer space had been added to the scope of CIP. The Commission on Space Management's Final Report, issued January 11, 2001, recommended that U.S. national interests include: the promotion of the peaceful uses of outer space; the use of the nation's potential in space to support its domestic, economic, diplomatic, and national security objectives; and the development and deployment of the means to deter and defend against hostile acts directed at U.S. space assets and against the uses of space hostile to U.S. interests.[34] Particular attention was paid to the role that commercial communications satellites play in the U.S. critical infrastructure and the need for more coordinated U.S. actions in various telecommunications-related forums (e.g., the International Telecommunication Union).[35]

NATIONAL DEFENSE, THE NATIONAL ECONOMY, AND CIP

National defense and the national economy are considered by many as the basic national security priorities. Institutionally, national defense security and national economic security are viewed as two closely related, but separate policy areas. This is illustrated by the establishment of the National Economic Council by the Clinton administration[36] and its continuation by the present Bush administration[37] to function alongside the National Security Council.

The two "securities" have become interrelated with CIP through two CIP-related Presidential Directives, an Executive Order, and a report by a Presidential Commission. Significantly, they were issued during the same time period that the other Commissions were developing and making known their findings and recommendations.

In mid-1996, an Executive Order created the President's Commission on Critical Infrastructure Protection ("PCCIP") to develop a comprehensive strategy to protect the following national infrastructures from physical and cyberattacks: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. These infrastructures "are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[38] A year later, the Report of the PCCIP highlighted the central role that these infrastructures play in "our national defense and our national economic power" and emphasized that their interlinkage via integrated telecommunications and computer systems, when combined with an emerging constellation of threats, has created a new dimension of vulnerability "of unprecedented national risk."[39] Presidential Decision Directive 63, issued in May 1998, established a framework for implementing the PCCIP's recommendations and again underlined the increasing reliance of the nation's military and economy on certain critical infrastructures and cyber-based information systems.[40] The present Bush administration's first National Security Presidential Directive ("NSPD 1") reinforced the view that national security "includes the defense of the United States, protection of our constitutional system of government, and the advancement of United States interests abroad" and "depends on America's opportunity to prosper in the world economy."[41] The Bush administration currently is preparing an Executive Order to implement NSPD 1. Thus, the development and implementation of CIP appears to be aligned generally with the relevant findings and recommendations of the other Commissions.

CONCLUSIONS

In revisiting our understanding of security from a CIP-perspective, the following conclusions, based upon the preceding discussion, should be taken into account:

- The redefinition of national security and of the national interest is evolving at both the theoretical and operational levels.

- The definition of the relationships between national defense security and national economic security policies and strategies is evolving.

- The definition of the relationships between CIP and national defense and national economic security needs to be agreed so that CIP-related national interests can be identified and articulated for consideration in the prioritization of this nation's overall national interests and the development of this nation's security policy and strategy.

- The identification of continued assurance of U.S. access to outer space for commercial and military use as a national interest has added a complex dimension to CIP.

SUGGESTED FRAMEWORK FOR A DIALOGUE

By providing a forum for a bipartisan dialogue, Congress can facilitate the redefinition of national security and national interest(s).

With respect to how to proceed, the preceding discussion of the theoretical and operational definitions of national security and national interest contain the elements of a bipartisan approach and are summarized below.

First, a special counsel to a former president has suggested that a narrow, not broad, definition of national security is required, and has proposed seeking to build a bipartisan consensus around a very limited number of basic national security goals, while leaving room for partisan disagreement on their implementation. National defense and the national economy would appear to be the logical candidates for these basic goals.

Second, the present national security adviser, before she assumed that role, has argued that American foreign policy should refocus the United States on the national interest and the pursuit of key priorities. Bipartisan agreement that national defense and the national economy are the nation's highest priority interests could enable further definition and prioritization of related national interests.

Third, bipartisan commissions have developed working definitions for national security and national interests in assessing the United States role in a changing global environment. They also have created a methodology for prioritizing these national interests and have applied the methodology to "the real world." Their findings could be utilized as baselines for the dialogue.

Dr. Jack Oslund is Professor of Telecommunication on the faculty of George Washington University's Graduate Telecommunication Program. His areas of specialization are in national security, international communications, and the impact of technology on domestic and international telecommunications policy. Late last year, he retired from the former COMSAT Corporation where, since 1974, he had served in a variety of management positions involving the U.S. Signatory role in INTELSAT and Inmarsat; he also was selected Chairman of the Legislative and Regulatory Group of the President's

National Security Telecommunications Advisory Committee. Prior to joining COMSAT, he served on the faculty of the Joint Military Intelligence College (formerly the Defense Intelligence College), was on the International Staff of the White House Office of Telecommunications Policy, and was an officer in the United States Marine Corps. In addition, he has been an Adjunct Professor in the International Communications Program of The American University's School of International Service. He received his Ph.D. in International Studies from AU's School of International Service.

Notes:

1. The Report of the Commission on America's National Interests, America's National Interests, July 1996.
2. The Reports of the United States Commission on National Security/21st Century, New World Coming: American Security in the 21st Century—The Phase I Report, September 15, 1999; Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom—The Phase II Report, April 15, 2000; and Road Map for National Security: Imperative for Change—The Phase III Report, March 15, 2001.
3. The Report of the Commission to Assess United States National Security Space Management and Organization, January 11, 2001.
4. The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (October 1997), p. ix.
5. Maxwell D. Taylor, "The Legitimate Claims of National Security," Foreign Affairs 52 (April 1974).
6. Jessica Tuchman Mathews, "Redefining Security," Foreign Affairs 68 (Spring 1989). See also Theodore Sorensen, "Rethinking National Security," Foreign Affairs 69 (Summer 1990).
7. Walter Lippmann, U.S. Foreign Policy (Boston: Little Brown and Company,1943) p.51. Cited in Arnold Wolfers, "'National Security' As an Ambiguous Symbol," Political Science Quarterly LXVII (December 1952), p. 484. See also Peter Mangold, National Security and International Relations (London: Routledge Press, 1990), p 2.
8. Wolfers, Ibid.
9. National Security Act of 1947 (61 Stat. 495; 50 U.S.C. 401).
10. Mathews, p. 162.
11. Robert Mandel, The Changing Face of National Security: A Conceptual Analysis (Westport, CN: Greenwood Press, 1994), p.37.
12. Mathews, pp. 162-177.
13. David Baldwin, "The Concept of Security," Review of International Studies 23 (1997), p.5.
14. Sorensen, pp. 6-7.
15. Wolfers, p. 481.
16. Fred A. Sondermann, "The Concept of the National Interest," Orbis 21 (Spring 1977). Today's debates are not between the realists and the idealists, but are between the neorealists and the neoliberals. See David A. Baldwin, ed., Neorealism and Neo-liberalism: The Contemporary Debate (New York: Columbia University Press, 1993), and Charles W. Kegley, Jr., Controversies in International Relations Theory: Realism and the Neoliberal Challenge (New York: St. Martin's Press, 1995).
17. Hans Morgenthau, In Defense of the National Interest (New York: Alfred Knopf, 1951) and Politics Among Nations, 2 ed. (New York: Alfred Knopf, 1954).
18. Condoleezza Rice, "Campaign 2000: Promoting the National Interest," Foreign Affairs 79 (January/February 2000), pp. 46-47.

19. Peter Trubowitz, Defining the National Interest: Conflict and Change in American Foreign Policy (Chicago: University of Chicago Press, 1998). Cited in Joseph S. Nye, "Redefining the National Interest," Foreign Affairs 78 (July-August 1999), pp. 22-23.
20. Morton A. Kaplan, System and Process in International Politics (New York: John Wiley & Sons, 1964), p. 151.
21. Commission on National Security, Phase II, p.7.
22. Commission on National Interests, p. 2.
23. Ibid., pp. 4-7 and 22-26.
24. Ibid,, p. 4 and p.22.
25. Ibid., p.51.
26. Ibid., p 47.
27. Ibid., p.54.
28. Commission on National Security, Phase I, p. 141 and p.143.
29. Ibid., pp. Phase II, pp. 5-6.
30. Ibid., p. 6.
31. Ibid., pp. 7-8.
32. Ibid.
33. Ibid.
34. Commission on Space Management, p. vii.
35. "Background Paper: Commercial Space and United States National Security" prepared for Commission on Space Management.
36. Establishment of the National Economic Council (Executive Order 12835, January 25, 1993).
37. Office of the Secretary, White House, News Release, March 21, 2001.
38. Critical Infrastructure Protection (Executive Order 13010, July 15, 1996).
39. PCCIP, p. ix.
40. Critical Infrastructure Protection (Presidential Decision Directive/NSC-63, May 22, 1998).
41. Organization of the National Security Council System (National Security Presidential Directive #1, February 13, 2001).

Counterintelligence and Infrastructure Protection

By John MacGaffin

THE BACKDROP

For years, it has been a given that "counterintelligence and infrastructure protection" could not be addressed in an unclassified forum. Parts of the defense and national security communities have consistently taken the position that public discussion of "the threat" and of our "defense" (to say nothing of our "offense"!), would give unacceptable advantage to those who would do us harm.

Whatever truth of that notion in the past (and it was not entirely without merit), it is increasingly wrongheaded today. In fact, just the opposite is true. The counterintelligence dimension of infrastructure protection urgently requires a new dialogue and new relationships among the defense and national security communities, the rest of the federal government, and some private sector entities. This in turn, undoubtedly, will require new policies—government and private—and, perhaps, new structures. If we fail in this, we will fail in a significant aspect of protecting our most important economic and national security interests.

Traditionally, counterintelligence has focused on *detecting* and *thwarting* threats posed by a finite number of *hostile intelligence services* to a defined set of (usually "classified") *national security secrets*. And during much of the past half century, that was entirely appropriate. Counterintelligence was practiced primarily by the Federal Bureau of Investigation, the Central Intelligence Agency, the Department of Defense, and the individual military services. Other government entities cooperated, but mostly under duress. To a very limited extent there was cooperation among the primary practitioners but, for the most part, they worked in their own sphere or "stove pipe"—the FBI concentrating on domestic activities, the CIA on events and players abroad, and the military on things military. These "stove pipes" did not talk to one another, and the private sector—other than defense contractors—was completely beyond the pale.

The elements necessary for defense (as well as offense) are almost certainly imbedded in that same information technology that facilitates the work of the spy. Critical infrastructures are, simultaneously, both the target for the "bad guys" and—if we can bring an appropriate new focus to the problem—the strength of our defense.

At our common peril, however, the situation is little changed today. Our counterintelligence entities—the FBI, CIA, and DoD—continue to focus primarily on the sources of traditional threats (the "finite number of hostile intelligence services") who seek to steal our traditional secrets ("national security information").

This is unacceptable because:

- Threats from traditional quarters (the intelligence services of hostile nations) are outnumbered today by activities directed against us by nations not normally regarded as hostile, as well as by non-state players such as terrorist organizations, international crime groups, and drug cartels. Put another way, today's threats are more diverse and complex than those we have faced in the "simpler times" of the Cold War.

- "Classified" national security information comprises only one element of what must be protected from both traditional and non-traditional quarters.

What we are doing today just won't meet the challenges of the future!

THE PROBLEM

Information technology, critical infrastructures, and counterintelligence are now inseparable. Information technology has become central to previously "traditional" counterintelligence problems—Aldrich Ames and Robert Hanssen succeeded beyond other traitors because IT facilitated their acquisition and transfer of critical information to hostile powers. What previously had to be done with a miniature camera in the dead of night, a micro dot, a dead drop, or Berlin Autobahn stop, can now be done by a key stroke or two.

The elements necessary for defense (as well as for offense) are almost certainly imbedded in that same information technology that facilitates the work of the spy. Critical infrastructures are, simultaneously, *both* the target of the "bad guys" and—if we can bring an appropriate new focus to the problem—the strength of our defense. Just as some hostile nations have already begun to develop advanced programs to destroy or incapacitate our major infrastructures, either as an element of war or as a covert means of enhancing their own economic position at our expense, we have begun ourselves to form our institutions and these technologies into the cutting edge defensive systems required. In fact, defensive systems need to be engineered into the programs as they are developed and deployed—not afterwards!

More importantly, however, our national/counterintelligence defense can no longer consist only of a 24 x 7 alert status to detect those who would do us harm. This was effective when the USSR, China, and a few others comprised the finite list of those who could do us significant harm. Today, however, this posture becomes our Maginot Line. If not altered significantly, "bad guys" will simply go around our defenses as the German forces did in France in WWI.

Finally, if U.S. National Security and Economic Security interests are coterminous—as at least three successive administrations have now declared—then it is clear that a government-centric view of the threat and of the defense (not to mention, yet again, the offense), will certainly miss the mark. The "Crown Jewels" of our National and Economic Security in the 21st Century are just as likely to reside in the private sector as they are to be the hidden "widgets" of some secret defense program in the bowels of the Pentagon. Indeed, the latter most often emerge from the former.

WHAT TO DO?

The Executive Branch, in full collaboration with the private sector, and with the enlightened guidance and encouragement of the Congress, must establish a national regime with the following attributes:

- Most important, the focus must be on deciding "what must be protected?" And since everything can't be protected, we must *establish a hierarchy* of "Crown Jewels." In its simplest form, we must identify and focus our attention on those things to which the description "unthinkable" would certainly apply were we to lose them.

- National Policy level input is the essential element in determining Crown Jewels.

- We must adopt a *proactive, not reactive, approach* to identifying those Crown Jewels and to formulating a *national level strategy* to integrate and focus our efforts.

- The new regime for counterintelligence and infrastructure protection—indeed for counterintelligence across all elements of national vulnerability—must *leverage all appropriate elements of the U.S. government.*

- The heart of leveraging, and its most thorny element, is *information, information, information . . .*

- The barriers to a significantly enhanced exchange of information across the traditionally uncommunicative stove pipes of government must be removed without advantaging our adversaries in the process.

- The tensions and barriers between the government and private sector must be replaced by a regime which permits collaboration while, at the same time, protects the secrets and proprietary information and privacy of both.

- The National Strategy must inform analysis, collection, and resource allocation across government and must form the basis for government-private sector interaction.

- Government must be accountable for performance against Nation Strategy and that accountability must be clear to the entire range of national policy level participants, not confined to the practitioners as it is today.

- The entire regime must be interactive—policy informs counterintelligence and counterintelligence ultimately informs the policy level of the state and health of the entire enterprise. And the process repeats . . .

- Put another way, if a new counterintelligence regime is truly effective, the Executive Branch, the Congress, and the private sector will all know whether we are, indeed, more secure than before.

CAN WE DO IT?

The good news is there are several new initiatives on the table which, if supported and nurtured by the Executive Branch and by the Congress, will constitute a major step in the right direction. Foremost among these is the National Counter-intelligence Executive (NCIX) created by PDD-75 under the Clinton administration and endorsed and implemented by the present administration. It has as its heart the identification of Crown Jewels across government and private sector, the formulation of National Strategy to organize the nation's efforts to insure the integrity of those Crown Jewels, the development of an analytic capability to inform both policy and operational levels of the state and health of the Crown Jewels and, finally, a system of accountability.

Within the Department of Defense, the present administration has established a Counterintelligence Field Activity (CIFA). The CIFA will integrate within DoD those functions now funded in various DoD CI programs to protect DoD personnel, operations, research, technology, and infrastructure from foreign intelligence services, terrorists, and other clandestine or covert threats. The CIFA will develop and manage the resulting integrated DoD CI program across those CI

missions identified in PDD-75. The heart of this Counterintelligence Field Activity is the Joint Counterintelligence Assessment Center (JCAG). Initially, the JCAG will focus on "horizontal protection"—that is, insuring that critical technologies in one DoD program are aligned with the same technologies in other programs. At present, such technologies may be closely protected in one program and released to other countries in another. When fully developed, the JCAG will provide a much more robust tool for DoD and the entire counterintelligence community, understanding and determining Crown Jewels beyond horizontal protection and informing DoD and national policy makers as to the state and health of those Crown Jewels.

Both NCIX and CIFA/JCAG embody the "attributes" of the regime described above. So far, other elements of the counterintelligence, security, intelligence and law enforcement communities have not taken similar concrete steps to move ahead. If we can take these first steps away from the world of stove pipes in which we have become so comfortable (and which has been so opaque to outside scrutiny), then we truly have a chance of getting out ahead of the more complex and more diverse threats we will face. If these, and other initiatives like them, are not established throughout government and private sector, we will certainly suffer.

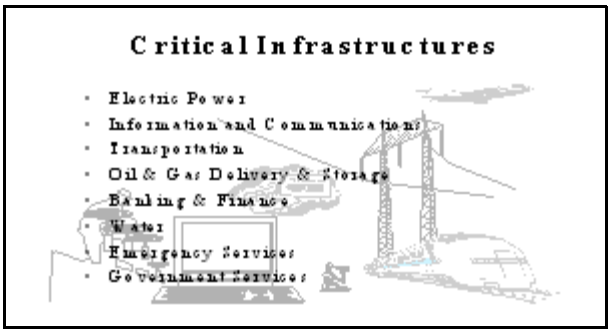
As one very wise member of the Senate Select Committee on Intelligence notes at the slightest opportunity: "We must stop looking only in our rearview mirrors."

A 30 year veteran of CIA, John MacGaffin served as Chief of Station in five countries, had responsibility for Strategic Planning and Evaluation for the Directorate of Operations, headed the Agency's Central European Operations Division, and retired as Associate Deputy Director for Operations. He served as Senior Advisor to the Director and Deputy Director of the FBI for five years. Most recently, at the request of the secretary of defense , the DCI and the director, FBI, he chaired the 18-month special review of national-level counterintelligence which resulted in PDD-75 and the implementation of the National Counterintelligence Executive. He is currently president of MacGaffin & Miller, Inc, a consulting firm in Washington, D.C.

Critical Infrastructure and Information Assurance: A Working Context and Framework

By Nancy Wong

A Working Perspective of Critical Infrastructures



Certain infrastructures deemed "critical" have been identified as essential to the nation's defense and economic security and the health, welfare, and safety of its citizens. Their incapacity or disruption could have a debilitating regional or national impact. Assuring these infrastructures and the information systems and networks on which they more and more depend for operations represents a complex and long-term undertaking. As anyone who works in these industries recognize, the work goes on every day, 24 hours a day, 365 days a year. There is no end date, and the assurance target moves. The drivers can be new markets, new threats, new technologies, or even new weather patterns.

To Whom Does It Matter?

The word infrastructure brings to mind a picture of wires, pipes, poles, and other physical structures. However, from a working perspective, the value and criticality of these "assets" are determined by how they contribute to the level and quality of service and product delivery capability expected by customers and the public. For some of the critical infrastructure industries, public expectations include rulings from regulatory bodies. Physical assets are just a part of a service capability; other parts include trained people and well designed processes. Consequently, many who own and operate critical infrastructures see what they do for a living as assuring the capability to deliver a critical service or product at the level of reliability, availability, and integrity expected by their customers and the communities they serve.

EXPECTED OUTCOMES

Owners and operators have been expected to assure delivery of critical infrastructure services for decades in many of these infrastructure sectors. Many of these services, as a result of responding to hurricane, flood, earthquake and other natural disasters, as well as to individuals with malicious intent, have developed a robustness and resiliency such that the average person takes them for granted. When we walk into a room and flip a switch, we assume the lights will come on. When we pick up a phone, we expect a dial tone. When we turn the tap, we expect drinkable water to flow. The expected level and quality may vary from community to community and from customer to customer, but in general, each infrastructure owner and operator has, more often than not, an explicit understanding of customer and public expectations. The consequence of not paying attention to these expectations inevitably leads to loss of customers, business and revenue, public embarrassment, and, for some, regulatory penalties.

Some highly interconnected infrastructures sectors, such as the electric power system and the banking and financial services system, have developed over years of experience a common understanding of customer and public expectations for the entire system, not just of the individual contributing parts. The development of industry structures such as the North American Electric Reliability Council (NERC), whose members and affiliates comprise just about all the participants of the electric industry, reflect the industry's understanding of the public's expectation of them. In the electric industry, it comes down to "keeping the lights on."

Each institution has an economic and public interest to assure its own services, including technologies on which those services depend. Disruptions of a large number of individual institutions can have an adverse impact on public confidence and economic security.

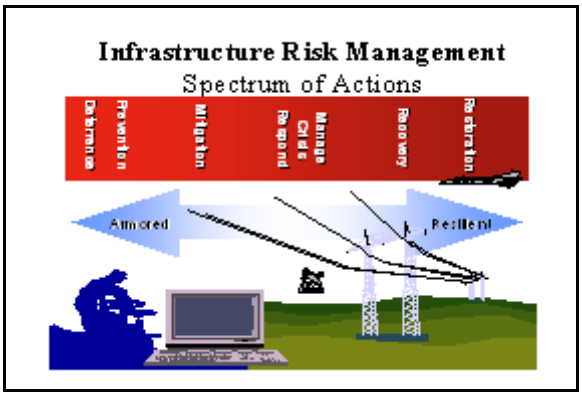
Assuring delivery of service is not only performing day-to-day activity well. It continually evolves with new customer or public expectations, new technology, new operating processes, new knowledge, and experience that comes from a wide variety of events that occur outside of the control of an infrastructure service delivery provider. The new element of concern is the emerging critical role of information technology systems and networks in delivering critical infrastructure services.

ASSURANCE THROUGH MANAGING RISKS

Assuring delivery of critical infrastructure services against disruption is inherently a risk management process. The variety and dispersion of physical infrastructure

components, human resources, geography, and possible causes of disruption are so diverse that 100% protection against disruption is neither affordable nor feasible. Assurance programs are planned, implemented, and executed by infrastructure service "operations" people, as an integral part of their day-to-day responsibilities, with goals set by implicit expectations or negotiated with their customers/users. Consequently, the assurance of any underlying critical support system, including an information network, is normally an integrated part of these assurance programs. The first challenge has been recognizing the role these underlying systems may play in core service processes. The second challenge is accepting that systems may be now subject to greater risk of disruption and the consequences of their disruption greater than ever before.

A Spectrum of Risk Management Processes



A complete and sufficient assurance program consists of elements from a spectrum of possible actions. Although terms of reference may vary from industry to industry, most well managed service or product delivery institutions manage their risks by investing in a form of each activity within the entire range. Risk is reflected by the level of consequence an institution is willing to manage and in how it decides to manage it, through varying levels of investment within this spectrum. Some institutions recognize and manage these processes explicitly. Many others do so intuitively. A service or product delivery institution can choose to do none of these activities. Then, implicitly or not, it has accepted the probability of going out of business when a disruption occurs.

Level of investment reflects implicit risk trade-offs based on what is known and what is affordable. When an institution cannot prevent or deter a disruption, it will attempt to mitigate the consequences to its service capability. What it cannot mitigate, it will respond by invoking procedures and resources to manage the crisis with its customers/users and restore its services, including, for some, the capability to reconstitute entire portions of its service infrastructure. Prevention or deterrence activities include employee education and awareness, corporate policies, and implementing security procedures and technology into service delivery systems as they are installed. Mitigation activities include service operations monitoring, analysis, and response to avoid a disruption. Crisis management and recovery include investigation, restoration, and sharing lessons

learned, the latter having potential feedback to improve all other activities of the assurance program.

In general, an institution will invest in a particular part of the spectrum based on several considerations:

- It invests in deterrence or prevention activities when:
  - Plausible disruption events are known and can be readily described.
  - Vulnerabilities can be identified and risks assessed.
  - Consequences can be identified and measured, even if only subjectively by management.
  - Effective tools, processes, and expected behaviors to prevent or deter:
    - Can be defined or identified.
    - Are readily accessible and available.
    - Are affordable.

- It invests in mitigation and response activities when:
  - Operation procedures can be well-defined; roles and responsibilities are clear.
  - Knowledge of operational base-line behavior, and meaningful deviations from that behavior are known and available.
  - Processes and tools are affordable and can be easily integrated into daily business operations.

- It invests in crisis management and restoration activities when:
  - Speed of restoration is perceived as a critical element to customer service and public confidence; outages happen.
  - Possible range of plausible disruptions or consequences cannot be predicted.
  - Adequate knowledge or experience from previous events is available to design effective crisis management or restoration procedures.
  - Cost of prevention or mitigation are not affordable or tools to prevent or mitigate disruptions are not easily available

In the latter category, managing public and customer confidence constitutes a critical component of a successful level of activity. Some service delivery institutions who, as part of their crisis management and restoration process, appropriately engage and help the public and customer/users manage possible consequences of a disruption have earned high marks for their service delivery capability.

Note that for each category, the availability of more credible information and experience, and greater accessibility to affordable tools and proven procedures encourage investments earlier in the assurance spectrum.

A Matter of Threat, Consequence Level, and Response

Just protecting an infrastructure against vulnerabilities and threats does not always correlate with meeting expected service outcomes. It will depend on the customer's or public's needs, options, and range of tolerance. Nor is zero vulnerabilities necessary as long as customer or user expectations are met. For example, some equipment fails every day in many infrastructures. Often, infrastructure service delivery continues, with the failure transparent to customers or the public because of the infrastructure service provider's planned investment in redundancy (prevention) or a by-pass process (mitigation).

Developing an Assurance Program

Institutions that deliver critical infrastructure services, in the main, take for granted what they do to assure those services. They "do" it every day by planning for and running their operations (and businesses) successfully. They tend to start their planning with the service delivery capability that defines why they are in business, the quantity, the quality, to whom, and for what purpose, as defined by customer or public expectations and tolerance for risk of the communities they serve. Each individual institution's understanding of new risks, their own tolerance for risk and the subsequent consequence also represents factors. Measures of operational success include reliability, customer/public satisfaction, responsiveness, efficiency (cost), and integrity of operations. No one program fits all.

Risk Assessment and Management: Making the Choices

Risk assessment identifies plausible threats, vulnerabilities, and potential consequences. Risk management consists of the spectrum of decisions made and actions taken to prevent, mitigate, or manage adverse consequences if potential threats become reality and exploit identified vulnerabilities.

Risk assessment generally includes the following steps:

- Identifying core service processes
- Identifying critical assets (including supporting information technology systems) that support those core processes
- Identifying the potential threats to and vulnerabilities of those critical assets

- Identification of the consequences (including costs) that will need to be managed if the potential threats were to exploit the vulnerabilities

Critical assets include more than physical components. They include all underlying services, people, procedures, supplies, and information systems that if disrupted or removed would have the effect of disrupting critical service. Vulnerabilities include lack of skilled staffing or operational procedures and documentation, as well as lack of secure information systems on which the critical service relies. Consequently, results of a risk assessment will tend to be unique to an individual institution and its operational business practices. Many risk assessments tend to be performed incrementally, and risk management actions implemented as a continuous improvement process.

WORKING WITH OTHERS TO IMPLEMENT

Current business processes have evolved over the last two decades, reflecting a global market place that is more competitive, fast moving, and demanding in quality. Public institutions have followed suit to a certain extent, driven by public expectations for more efficient and effective operations and use of the tax dollar. Institutions focus on core competencies and look to others to provide services that are not central to the core mission. Traditionally, private institutions have looked to government for certain services, such as law enforcement, national defense, and coordination for disaster relief. They also look to others to provide essential services that are far more efficient for others to provide. As a result, the implementation of the assurance process includes the planning, development, and coordination of relationships with third parties as part of the risk management process.

Peer Relationships

Some sectors have formal or informal agreements among its members. These agreements serve to coordinate activities and share limited resources, in order to assure reliability of their national infrastructure and provide adequate response to a crisis within the communities they serve. The development of information sharing and analysis centers (ISACs) within the sectors, oftentimes, just formalizes and broadens the sector reach of what may be informal arrangements between individuals to share information. As such, ISACs represent another means to help manage service risks of the participants and their infrastructure. In the area of recovery and reconstitution, for example, electric companies have mutual aid agreements to dispatch crews, across the country if necessary, to restore and rebuild electric infrastructure damaged or destroyed by natural disaster or other causes.

Government Relationships

Many critical infrastructure institutions work closely with their local and state emergency response agencies. Their emergency response, recovery, and reconstitution plans are usually integrated and priorities set with those of the local and state emergency response plans. In regions subject to many natural disasters, disaster drills are common annual or semi-annual practice for individual institutions. If the industry is regulated, institutions also work with regulatory bodies to assure adequate funding for these processes and to assure review that the processes are adequate from a public perspective. The objective is to reduce loss of life and property and restore service as quickly and effectively as possible.

Most of the infrastructure sectors also work closely with law enforcement to respond to incidents of infrastructure disruption. Disruption of a critical infrastructure service may itself be a criminal act, but the confusion surrounding an event can also create opportunities for criminal activities. Reporting crimes to law enforcement for prosecution also provides a deterrence value. Law enforcement in turn has developed various channels to warn institutions of new threats or possible attacks.

Supplier and Customer Relationships

Institutions look to their suppliers for necessary services and products to perform their daily business of delivering service, at times incorporating reliability requirements into service agreements. They may develop requirements to assure service in time of crisis or they may develop contingent means of supply. They may include the service or product supplier in their contingency and restoration planning, if the service or product is recognized as critical to sustaining or restoring operations.

Over the last decade, the quality of customer service has emerged as a differentiator, and many times for regulated institutions, a regulatory requirement. An important component of service assurance is communications and education for customers and the communities that the institutions serve, both for public safety and to maintain public confidence, particularly in face of a major regional disaster. Communications and education include counsel to customers on how to prepare for a major outage to systematic updates and information on progress of restoration. For larger customers who might incur substantial risk to either life or property if disrupted, the service provider may work with them to develop contingency plans. These activities are recognized as good practice no matter how an outage or disruption occurred.

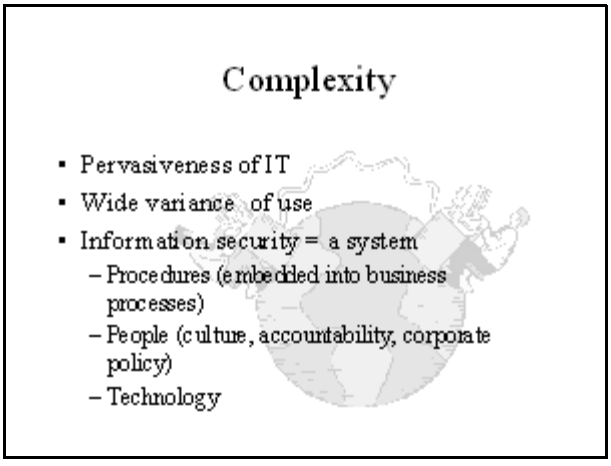
INFORMATION ASSURANCE IN CONTEXT

What is new about assuring critical infrastructure services today is their reliance on information systems and networks and the emerging risks associated with their security. Change is escalating in all critical infrastructure industries. Business processes are evolving as fast as the technology that can support them. "Just in time" delivery and customer service processes are the norm rather than the exception and represent a base line for many operations. Industries are being restructured as market and customer expectations change driven by a global economy. E-government services provided unprecedented access and efficiency. Consequently, a service or product delivery institution more and more must also assure the availability, reliability, and integrity of information and networks critical to that delivery.

Assuring the information infrastructure used within an institution is also a risk management process. Information assurance in general is concerned with the availability, reliability, and integrity of information systems. It includes continuity of operations, under a wide variety of circumstances including natural disasters and accidents. It also includes information security. Earthquakes and floods have been known to take out information technology systems for long periods of time. The possibility now exists that individuals with malicious intent can do the same. The planned action to restore a critical infrastructure service would include what to do if information systems become corrupted or unavailable, no matter what the cause.

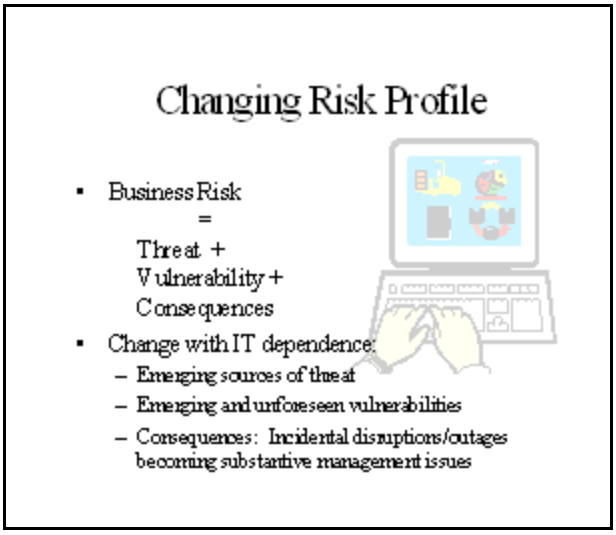
Some Differences

Information systems as an underlying "critical asset" exhibit a unique set of characteristics. Operational dependencies will vary so risk profiles will vary, sometimes dramatically, depending on how information is used within an institution. The type of technology and its applications can vary dramatically from sector to sector, and from institution to institution. There are a wide variety of information technologies in use. The same technologies can be used in very different ways, some probably unimagined by the original developers. Consequently, information assurance and security programs tend to be highly tailored.



They have to fit within the processes, the culture, the managerial framework, and the technological choices made within individual institutions and industries. Information (or cyber) security, like a padlock, has no intrinsic value in itself to its owner. It assumes a value commensurate with the value of what it secures or the cost of a situation it is designed to avoid. Consequently, information security requires a meaningful context for successful recognition, acceptance, and application.

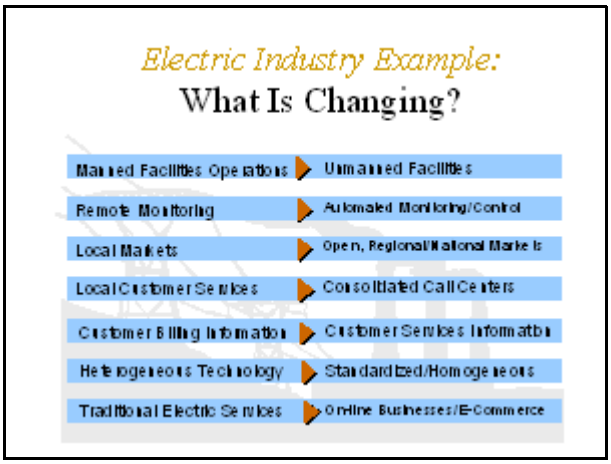
Ubiquitous Ownership and its Implications for Security



The source of threat to information systems can come from anywhere, oftentimes from outside of a service territory. The threat continuously evolves and evolves at an unprecedented speed. It is no longer a matter of "if" an attack on a network may happen. It does happen, and with great regularity, as we have seen within the last several years.

The ubiquity of ownership and access to fairly sophisticated information technology by anyone with limited technical knowledge opens up a whole new range and volume of possible exposures for every information system and network that is in anyway connected to others. The ease of use and availability of tools for mass disruption makes everyone more dependent than ever before on each other for "safe and secure" operations.

Addressing the National Interest



From the national perspective, addressing the issue of assuring critical infrastructure services requires multiple levels of attention with different types and levels of activity. It will be a continuing process involving the infrastructure sectors to do what

they "do" to assure their services, incorporating the new dimension of information technology dependency.

THREE LEVELS OF ASSURANCE

Each institution has an economic and public interest to assure its own services, including technologies on which those services depend. Disruptions of a large number of individual institutions can have an adverse impact on public confidence and economic security. Awareness building and education for understanding the emerging threats and vulnerabilities and their potential consequences represent a critical first step. Translating the issue into relevant terms for industry will surface the requirements that will shape demand to drive market solutions. At the same time, obstacles can be identified that may need support to remove.

Secondly, many of the critical infrastructures consist of highly interconnected and integrated facilities and operations, which together constitute what the public sees as the sector's "national infrastructure." Examples include the electric power and telecommunications systems. Each of these critical infrastructures depends on members of their sector working together to assure the reliability and smooth functioning of highly integrated operations. The objective is generally to assure reliable operations of the entire connected system and to prevent disruption or outage in one region or area from cascading into another. The federal government traditionally has encouraged this national level cooperation when it deems it necessary to serve the public interest. With the dependency on information networks to run critical infrastructure operations, a new layer of interconnectedness and integration is now emerging. It will require concerted attention and action to assure that disruptions to networks supporting one part of the infrastructure system do not cascade and disrupt other parts. Again, understanding of this new dependency and its new risks is a critical first step to encourage critical infrastructure sectors to incorporate information network security considerations into their service operations.

Thirdly, for each infrastructure, dependencies on other critical infrastructures for services have grown over the last decade. In disrupting a national infrastructure, the effect of such dependencies has yet to be understood. Because of its complexity and lack of market drivers, an initiative to address infrastructure interdependencies will likely need support from the federal government if it is to be addressed at all.

A CONTINUOUSLY EVOLVING PROCESS

The Year 2000 information technology conversion had a "hard" end date. One of the challenges of critical infrastructure and information assurance is that it does

not. From a working perspective, the general principles of critical infrastructure assurance include information assurance as part of assuring critical services delivery. Those principles also apply to information assurance when it is identified as a critical asset. The problem and the solutions will continue to evolve along with technology, business processes, and the imagination of perpetrators to create new tools of disruption. As a result, like "public safety," managing information security risks of critical infrastructure will evolve and necessarily become a core management practice to deliver a critical infrastructure service.

Nancy Wong currently serves as a senior executive and program manager for industry outreach in the national Critical Infrastructure Assurance Office of the Department of Commerce. Ms. Wong served as a commissioner in 1997 on the President's Commission on Critical Infrastructure Protection as a private industry representative, with experience in both the energy and information technology industries. She took a leave of absence from her position as department head for information assets and risk management with Pacific Gas and Electric Company, where she oversaw the development and implementation of corporate policies, standards, and business processes to manage and protect the company's information technology assets. From 1993-1996, Ms. Wong led PG&E's 900-person corporate computer and network operations department. In this position, she managed an annual budget of $60-80 million and the planning and daily operations of the company's entire corporate computing and telecommunications infrastructure, one of the largest private networks in the country. Ms. Wong was selected as one of the "Top One Hundred Women in Computing for 1996" by McGraw-Hill Publishing Companies.

Ms. Wong holds a master's degree in finance and a bachelor's degree in computer sciences and mathematics from the University of California at Berkeley.

Information Protection: Assuring Stakeholder Value in a Digital Age

By Michael Rasmussen

THE NEED FOR INFORMATION PROTECTION: OUR PRESENT SITUATION

Ten years ago, many of the walls of communism fell; little did anyone comprehend that this event would be dwarfed in proportion by the fall of global communication barriers that the Internet has brought down. Whatever an individual wishes to call it—the Digital, Information, Knowledge, or Internet Age—the world has seen a dramatic shift in the way business is conducted.

The proliferation of networks, and with that the Internet, has evolved global communication. Organizations and consumers now have instant access to information—information that provides the knowledge needed to make better decisions. Enhanced communication and knowledge allows for increasingly agile organizations that are quick to respond.

Just as major events such as earthquakes, floods, and volcanoes have the power to change the physical landscape of the earth, technology has impacted the political, legal, competitive, and protective landscapes that surround us.

In the past, organizations have been secure behind their physical walls—walls that provided adequate security to protect assets. Today, these walls no longer provide protection, since access to organizational assets is available electronically. This has reengineered the way business is conducted; no longer is an organization a self-contained unit. Communication and access to internal knowledge is easily accessible to internal employees, business partners, remote offices, consumers, and even competitors.

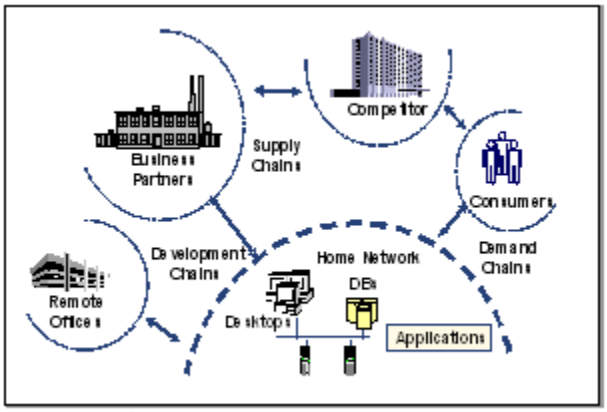


Figure 1: Organizational Security

Typically buried in the information technology department, the openness of today's business environments has escalated the need for information protection to the highest level of organizations, entire industries, and even governments.

DEMANDS ON INFORMATION PROTECTION

Two years ago, it was common to pick up a trade journal and not see an article on information protection. Today, business, as well as technical, journals are riddled with the issues surrounding the need to secure information. Awareness has grown, resulting in ever-increasing demands on organizations to provide adequate protection of their systems and the data contained therein.

The assault on systems is typically stereotyped as the teen-age hacker who wants to wreak havoc on organizational data. While there is a minor threat in this type of hacker, it is far from being the most significant threat organizations face. Individuals perpetrating security violations come from many walks of life. A threat might be an employee with malicious intent, an industrial espionage agent hired by a competitor, a foreign government desiring economic advantage or even a cyberterrorist out to cause mass disruption.

Organizations of all sizes and industries are targets. Every organization has the potential of a malicious employee, the hacker who wants to overcome a challenge, activists who want to display their propaganda, or the skilled cyber-thief who wants to use other systems to launch an attack. In the spring of 2001, the world watched an unsanctioned "hacking war" between China and the United States. The basis for this war was increased political tensions as a result of a plane collision near Chinese air space. It did not matter what your organization did, you were a target of the hackers on the opposing side.

Figure 2: Increasing Pressures—It's Not Just Hackers

The myriad threats organizations face have resulted in increasing points of pressure on organizations that mandate the appropriate protection of information. Consider the following:

Legal — Organizations face increasing legal pressure forcing them to take precautions to protect their systems. Chief among these pressures is the threat of

legal liability. Predominantly, attacks do not originate from an attacker's location. Instead, attackers typically weave their way through compromised systems before launching an attack. Downstream liability results when a victim is attacked due to another organization's negligence in securing their systems.

Insurance — Many organizations look to cyber-insurance to help mitigate the threat should they experience a loss or lawsuit due to a security incident. Insurance companies often gauge premiums on the organization's information protection program. It is typical for insurance companies to validate that an organization's information protection program meets a set of stated requirements before providing insurance to the organization. As more organizations look to insurance to minimize potential losses as a result of a security incidents, they will be forced to implement a solid information protection program.

Regulations — Government has become increasingly involved in mandating security controls on specific industries, as well as government institutions themselves. Of specific interest is the need to secure critical infrastructures of a nation—transportation, finance, utilities, communication, and health care. These vertical industries offer key threats to national interest should they be attacked with resulting data loss, manipulation, theft, or DoS. The U.S. government has formulated the National Infrastructure Protection Center to facilitate the protection of these industries. The U.S. has also enforced security through regulations, such as the Health Insurance Portability & Accountabilty Act (HIPAA), targeting health care and insurance companies, and the Gramm Leach Bliley Act (GLB), targeting financial institutions.

Just as major events such as earthquakes, floods, and volcanoes have the power to change the physical landscape of the earth, technology has impacted the political, legal, competitive, and protective landscapes that surround us.

Consumers — With concerns of theft of credit card information and identity information, consumers want to be assured that their data is being properly secured. Providing encryption of Web pages via the lock or key in the corner of a browser does not provide security if the Web server itself has not been adequately secured. An attacker is more profitable attacking the server where the data resides and obtaining thousands of credit card numbers than trying to decipher the encrypted communication from one browser session.

Privacy — Closely linked to other consumer concerns, privacy has reached a paramount importance among individuals. Government has regulated privacy through HIPAA and GLB. Individuals want to know and be able to control how their data is handled. Privacy does not happen in a vacuum; enforcing a privacy

policy requires that an information protection program be in place to support the policy.

Competitors — As organizations face increased competition—not only locally, but around the world—the threat of industrial espionage increases as attempts are made to gain competitive advantage. Through organization reengineering, resulting in the increased dependence on business partners, organizations face a greater threat from business partners that might be servicing competitors.

Cyberwar — Governments and terrorist groups around the world are developing cyberwar capabilities. Should hostilities arise, not only are the physical assets of a nation open to attack, its electronic systems lay open for attacks as well. Targets of specific interest are critical infrastructures that can significantly affect the operation and trust of the systems they rely on.

Business partners — It is not uncommon for a business partner to have network connections to an organization and its competitors. With weak security controls, it can be a simple step to use the business partner as a doorway into a competitor. Many organizations are requiring security audits of potential business partners before allowing their systems to be accessible to the other.

Wall Street — And then there are stakeholders of an organization. The need to secure data for the benefit of stakeholders sums up all of the other demands of information protection. Stakeholders in an organization are interested in seeing a return on their investments and that their investment is adequately protected. By the nature of the word "stakeholder," they represent a critical concern that the organization is successful. Through loss of operations, bad publicity, customer loss, or trade secret theft, the value of the organization can be adversely affected, resulting in a lack of confidence in returning stakeholders.

WHO IS RESPONSIBLE FOR INFORMATION PROTECTION

Historically, information protection has been delegated to the depths of an IT department. It seldom poked its head out to the rest of the organization as long as no significant events transpired. This is no longer the case.

To adequately protect stakeholder value, organizations need to take the responsibility of information protection from the top down, consider:

1. Board — Represents the body ultimately responsible for protecting stakeholders within an organization. Information protection should be a critical oversight requirement of an organization's board of directors.

2. Executives — The most senior level of management accountable to the board of directors. Executives are responsible for the ongoing management of the organization and should be fully supportive in the development of information protection mechanisms. The chief security officer is the executive primarily responsible for information protection.

3. Managers — Responsible for communicating information protection policies to those they manage and providing a liaison back to management regarding the effectiveness of policies.

4. Employees — Represent the strongest mechanism to securing information. With access to critical data in their jobs, security suffers if they do not know what is expected of them to protect this data. It is critical that employees are fully aware of how the information is to be protected.

5. Business partners — With the increased dependency on business partners, it is critical that business partners understand and adhere to an organization's information protection policies. All business partners should be educated on the responsibilities expected to protect the data of the organizations they work with.

MANAGING RISK—WHAT LEVEL OF SECURITY IS APPROPRIATE

Defining Risk

There are those individuals who approach information protection with the "impenetrable fortress" mentality, an approach that is impossible to maintain and that does not make business sense for the average organization.

It is impossible to obtain perfect security—every organization is going to have some point of vulnerability. Further, it is not economical for a business to provide an ultra secure environment. There is such a thing as "good enough" security, although it is a concept that can only be obtained by a defined and functioning information protection program.

Effective information protection begins with risk management. Risk management involves understanding the risks to an organization and managing them appropriately. This starts with understanding the risks an organization faces with the loss of availability, theft, or corruption of its data and analyzing it against the likelihood of an event happening, with the subsequent cost to the enterprise. Only then can an information protection program make sound business decisions to deal with the risk.

When risk is identified, there are three options an organization can take to manage the risk:

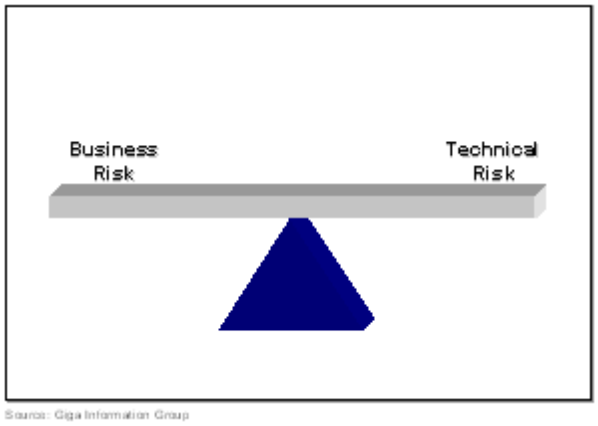
1. Insure the risk through the acquisition of an insurance policy should a negative circumstance be encountered.

2. Reduce the risk with an application of cost-effective countermeasures that mitigate the risk.

3. Accept the risk; not all risk can be cost effectively insured or reduced, forcing organizations to accept a certain amount of risk.

The key here is that organizations have to accept some level of risk. What level of risk is appropriate is the delicate balance that organizations need to maintain. This balance is a moving target in today's world.

With the increasing pressures on information protection previously mentioned (e.g., legal, insurance, regulatory, etc.), what was an ac ceptable level of risk in the past is now unacceptable as the pressure to protect information has increased from many angles. No longer can many organizations afford not to practice some form of security maintenance (e.g., applying security fixes to systems), with the recent rise in attacks and the surmounting legal liability and insurance costs—it is no longer an acceptable risk. With the advent of many regulations, certain industry sectors now face fines and even prison sentences if information should be compromised—a risk they are not willing to take that, in turn, forces stronger security.



Source: Giga Information Group

Figure 3: Balancing Risk

A confusing issue in information protection is the difference between business risk and technical risk. For an organization to effectively manage risk, an understanding between their differences and the impact on an organization is mandatory.

Technical Risk — Involves the risk an organization faces due to an exposure on a system. An exposure could be many things, including the following:

- A vulnerability in software that, when exploited, can give a remote attacker full access to the system or its data

- A weak password to an account on the system or a password taped to a monitor

Software vulnerabilities are continuously discovered. A system that appears to be fully secured can be wide open to attack the next day because a new vulnerability is discovered.

Purely fighting technical risk is a losing battle. The "impenetrable fortress"-minded individuals gauge security by technical risk in which they feel a mandate to eliminate every vulnerability discovered.

Business Risk — Deals with the risk a business faces should a technical risk be exploited by an attacker. However, evaluating business risk involves understanding the impact on the organization as a result of an attack.

Two systems that have the same technical risk, often have varying business risk. Exploiting a vulnerability on a server that is set up to test a new Web site has a lower risk than the same vulnerability being exploited on a system housing the organization's financial systems.

Evaluating business risk requires an understanding of technical risk, but goes beyond the technical to understand the actual risk impact on the organization. Business risk analysis builds on what is discovered in technical risk analysis.

The successful information protection program relies on understanding technical risks as they are measured by business risk. Only in light of business risk—discovering the likelihood and impact the organization faces to a threat—can an educated decision be made on how to deal with the risk. If it would cost more to protect the organization from the threat than the impact the threat has on the organization, the protection mechanisms do not make sound business sense.

Both technical and business risks are ever-evolving. A risk that was acceptable last year—due to regulatory penalties, legal pressures, or a rise in industrial espionage concerns, among other circumstances—may no longer be acceptable. An ongoing process to manage risk is the key to gauging what level of information protection is appropriate.

How Due Diligence Factors Into Risk

Due diligence, in regards to information protection, involves assuring that adequate controls and processes are in place to protect an organization's systems. Without measurable guidelines, however, due diligence is relative and will vary from organization to organization—and for that matter from individual to individual within an organization.

In the past, due diligence, to many, consisted of installing a firewall between the organization's internal network and the Internet. This is no longer the case. *The increased risks businesses face from attacks, legal liability, insurance requirements and regulations mandate organizations take a more proactive stance in managing information protection.*

Beyond deploying a firewall, organizations need to adopt policies, processes, and supporting technologies that provide a defined level of due diligence. Organizations need to take a holistic view to their information protection program that is integrated into the overall environment.

Responsibility for due diligence starts at the top of an organization with the managing executives and moves down to the bottom. Executive management needs to define what level of risk is appropriate, how that risk is to be managed, and what standards for measurement will be put in place to protect information. The information systems department is responsible for seeing that adequate and cost-effective technical controls are put in place in organizational systems. Managers are responsible for seeing that their employees understand what is expected of them in protecting information. Employees are responsible for the day-to-day protection of information their position allows them to come in contact with and how it is used within and without the organization.

Validating Compliance—The Future of Information Protection

The issue remains—how does one measure what level of due diligence and, for that matter, risk is appropriate?

Government has answered this for specific industries through regulations. HIPAA and GLB have information protection components that define what is expected of organizations in those industries. This sets a standard by which to measure due diligence. However, regulations are not always comprehensive or clear in *how* to protect information.

Many industry sectors do not face regulations that mandate a set of security controls at this time. What do they measure their information protection programs

against? The answer lies in adopting a set of standards/practices defined and recognized by many to measure an information protection program against.

The defining standard for developing an information protection program around is ISO 17799, formerly British Standard 7799. ISO 17799 provides a framework to build an information protection program around. Beyond ISO 17799 and government regulations, other standards and best practices exist throughout the world that organizations may adopt.

The future of proving a level of due diligence has been adopted within an organization will be measured by validating compliance to standards and regulations. Consider the following:

- If an organization desires to obtain a cyber-insurance policy, validating compliance to information protection standards will be used to measure premiums.

- In a legal defense case, where a system was compromised and used to attack another party, the ability to show that standards were adopted and applied consistently to protect information will form the basis for a defense of due diligence.

- For the organization looking to attract investors, proving compliance to industry standards goes a long way in assuring future stakeholder value in our digital age.

DEVELOPING AN INFORMATION PROTECTION PROGRAM

The Building Blocks to Information Protection

In the past, organizations have continuously approached information protection through the acquisition of products, such as a firewall. Many have failed in this approach to information security since they have been left vulnerable to attacks that a firewall does not adequately protect from. Consider the following:

- Many attackers today attack the application running on a system, which is a method of attack that few firewalls can protect against.

- Security professionals have often labeled networks as being hard and crunchy on the outside and soft and chewy on the inside because of firewalls—they do not protect organizations from one of the most significant security threats: internal users.

Organizations added other products to try to overcome the issues left by firewalls, one being intrusion detection systems. These systems promised the ability to detect attacks, but organizations failed to realize the complexity of and commitment these systems required and the fact that they are what they say they are: *detection* systems—not *prevention* systems.

The approach of providing information protection through products is prone to failure. In fact, many security professionals have long stated, "Information security is a process, not a product!" Instead, organizations need to build a solid understanding and foundation for developing an information protection plan.

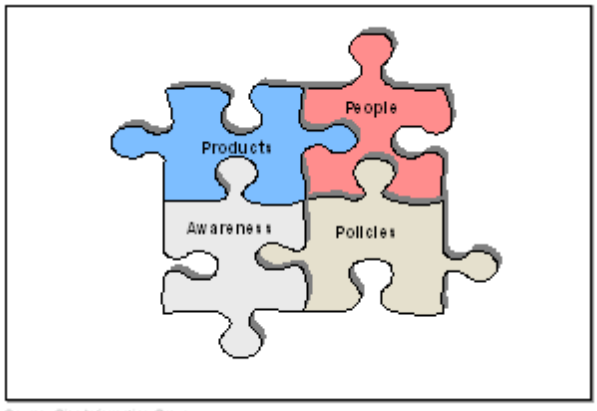
An information protection program is built on the understanding of two components: (1) understanding the process of information protection and (2) defining a plan to lay out an organization's information protection plan.

The Process Components of Information Security

Organizations are often composed of processes. An organization might have a business development process, a manufacturing process, or a research and development process. Each process can consist of subprocesses, which together contribute to the whole.

Information protection is the same—it can be seen as a process within the organization. In fact, the most successful information protection programs are the ones that view it as a process and manage it accordingly. In order to develop an information protection plan, it is essential that the process be clearly understood.

Processes consist of components; likewise, the information protection process has its components. To understand the information protection process requires an understanding of the components it is built on—only then can a clear plan to an information protection program be put in place.



Source: Giga Information Group

Figure 4: Keys to Information Protection

The following four components are used to build the process of information protection:

1. Policies — State the organization's objectives, purpose, and measurement requirements. Policies, in this case, represent a broad term that encompasses

policies, standards, procedures, and guidelines. These documents represent the foundation on which the process is defined and built around.

2. People — Assigned the task of fulfilling the responsibilities stated in the governing policies. The category "people" can represent all employees of an organization since they are given the responsibility to protect the organization. More specifically, people can represent the information security professionals who are devoted to the task of managing risk and implementing technical controls.

3. Awareness — A key component of an intrusion protection process in which individuals are consistently and actively communicating their role and responsibility to protect the organization's data. Awareness involves ongoing training for technical staff so it is clearly understood how they can protect the systems they are responsible for, as well as for end users in an organization who need to understand how to handle the information they come in contact with.

4. Products — Select products that complement the environment. Applying technologies for intrusion protection is not done blindly, but involves understanding the objectives and risks to the business and deploying effective technologies to reduce risks.

Once an organization understands these four fundamental components of the information protection process, a plan can be developed to see that an adequate level of protection is obtained.

Seven-Step Plan to an Information Protection Program

An effective information protection program is unique in every organization since it is tailored to the company environment, industry demands, and organizational goals. Organizations have different needs and demands to see that their information is secure. These might be related to industry requirements, such as regulations, the sensitivity or value of the information the company possesses, or the company culture itself.

However, common steps can be seen among organizations that differ in their approach to information protection to build an effective program around.

To define a plan for an information protection program requires an understanding of the components of the information protection processes previously stated: policies, people, awareness, and technologies. With an understanding of the importance and interrelation of these components, the program plan can be clearly

defined. Each component is to be addressed through the progression with a program plan.

While there are many approaches to developing an information protection program, the seven-step plan illustrated in Figure 5 is given as a solid foundation to build on.

Each layer in the plan builds on the layer it resides on; thus, lower layers provide a foundation for the layers above them. It is important that organizations adopting this plan build each layer on the preceding layers, since success depends on understanding the previous layer.

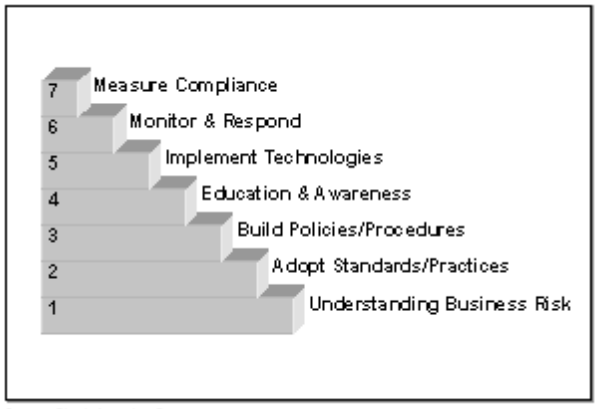


Figure 5

Following this plan will deliver a successful information protection program that addresses the organization's needs. This is a program that does not blindly throw technology at the problem, but one that is measurable and allows an organization to cost effectively manage risk.

1. Understanding Business Risk

As previously mentioned, information protection is about risk management.

Every organization is unique in the way it interprets risk. How much risk is acceptable depends on an organization's industry, the value of organizational information, company culture, and the willingness of management to accept risks.

Without gaining an understanding as to what risks an organization faces, along with what level of risk that management is willing to accept, it is impossible to develop an effective information protection program. It is akin to throwing a jigsaw puzzle in the air and hoping it lands with every piece in its proper place.

Understanding the risks a business faces, along with what level of risk is acceptable, allows information protection professionals to implement the appropriate and cost-effective safeguards and to combat risk. This lays the foundation that a solid information protection program is built on.

2. Adopt Standards & Practices

Once an organization understands the risk it faces and what it is willing to accept, the next step is to adopt recognized standards and best practices to build the program around.

With increasing pressures on information protection from legal, insurance, government, and stakeholders, it is necessary to integrate recognized information protection standards. The adoption of recognized standards provides a baseline against which the program can be measured and validated for compliance.

Since understanding business risk provides a foundation, standards provide the framework that lies on top of that foundation and defines what the program looks like.

The defining international standard for an information protection program is ISO 17799, which provides a thorough structure for a complete program. Other standards and best practices can then be adopted to provide more granular detail where needed.

3. Build Policies & Procedures

An effective information security program requires a clear understanding of expectations. Individuals, whether information protection professionals or the receptionist at the front door, need to clearly understand what is expected of them to protect an organization's information.

Polices are a set of documents that define information protection expectations. Policies are broken up into four functional areas:

- Policies: Policies are high-level statements that provide a framework of expected and mandated behavior of workers, management, technology, and processes. They include instructions, procedures, courses of action, and principles of guidance that are mandatory within the organization.

- Guidelines: Guidelines are optional and recommended behavior of workers, management, technology, and processes. The difference between many policies and guidelines is the use of words such as "shall" in procedures being replaced with "should" in guidelines.

- Standards: Standards outline specific technologies and processes within an organization, such as implementation steps, systems design, operating systems, applications, interfaces, and algorithms.

- Procedures: Procedures are a list of detailed and outlined steps of a specified process that individuals must employ while conducting the process. These may outline the destruction of sensitive information or how to respond to an attack.

Organizations support the framework of standards adopted by developing the policies, guidelines, standards, and procedures that state how information is to be protected in the organization's environment.

4. Education & Awareness

For policies to be effective, it is mandatory that they be communicated. Individuals cannot be held accountable if they were never aware of what was expected of them.

An effective information protection program is one that actively and continually communicates policies. A concept promoted by one vendor, PentaSafe, is the "Human Firewall." This concept involves ensuring that individuals know what is expected of them and how they are to go about complying with these expectations.

The majority of attacks involve an insider to an organization—often naively. Insiders who know how to appropriately manage and protect the information they come in contact with provide the best defense for an organization.

5. Implement Technologies

Security technologies are not to be randomly implemented. Instead, security technologies are to be selected as they cost effectively combat organization risk and are in line with adopted standards and policies.

Many organizations will implement a security technology based simply on what everyone else is doing. Everyone is buying a firewall, so an organization goes out and buys a firewall; everyone is buying a state-of-the art intrusion detection system, so an organization goes out and buys a state-of-the-art intrusion detection system. This is the wrong approach.

First, organizations need to understand what technologies appropriately combat their risk. Second, they need to understand how these technologies will be implemented and maintained (e.g., standards, policies). Only then can the product be selected that best meets the needs of the organizational environment.

Technologies are to be implemented that specifically combat organizational risk and are in line with standards and policies that the organization has adopted.

6. Monitor & Respond

The next step in an information protection program involves enforcement. Systems should be monitored for security incidents, and when an incident is identified, the appropriate response is to be initiated.

Monitoring and response put the teeth into the information protection program. It does not make sense for an organization to develop an information protection program, prepare and communicate policies, and deploy security technologies if security violations are going to be ignored.

The effective information protection program involves monitoring for security incidents and responding to identified incidents. If an organization continuously ignores security violations, it is difficult for that organization to respond to an incident in the future.

Internal employees can become lax in their enforcement of policies and management of technologies if they know that management is not behind those policies in seeing that they are followed through. This makes it easy for malicious attackers to use this to their advantage as the organization's guard is let down over time. To combat this, regular monitoring of the information protection policies and technical controls needs to be in place and significant incidents that represent a violation responded to.

7. Measure Compliance

To validate that an information protection program is working according to adopted standards and governing regulations, it is necessary to measure compliance to those standards on a consistent basis.

With increasing legal, insurance, and regulatory pressures, validating ongoing compliance will become a regular process for many organizations. Organizations will have to prove to others that their information is secure. In the future, more pressure will be put on organizations to validate they are effectively managing the protection of their information.

To manage this process, organizations need to adopt processes, technologies, and services that will regularly measure compliance of their information protection program. Where gaps in following standards are found, organizations must correct that gap so they maintain compliance with standards and regulations.

Beyond outside pressures, measuring compliance to standards provides for a strong information protection internally to the organization. Left unsupervised and not reviewed for compliance and effectiveness, a process can easily become inefficient.

Michael Rasmussen, a Certified Information Systems Security Professional (CISSP), is an analyst for Giga Information Group covering information security. An information security professional with more than 10 years of experience, his area of research includes the following:

- *Understanding and promotion of risk analysis methodologies*
- *Enterprise security architecture design and implementation*
- *Intrusion management*
- *Information protection standards and regulations*

Mr. Rasmussen's expertise ranges from risk analysis and policy development to the technical aspects of managing incident response, security assessments, intrusion detection, and security architecture design. During his career, he has worked in both the consulting and enterprise sectors. Mr. Rasmussen is currently the president of the Information System Security Association (ISSA) Milwaukee Chapter and has been involved with the ISSA International Board in various functions. He frequently speaks at information security seminars in which his broad experience allows him to cover all aspects of information security with a unique blend of both the technical and business perspectives.