

Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts

by

John A. McCarthy, Maeve Dion, Olivia Pacheco, & Chris Burrow

Published in [Cyberpower and National Security](#) (Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., Potomac Books, Inc., 2009), p. 543.

In this chapter, we examine the cyber infrastructure of the United States, which has become vital to national defense infrastructures, the U.S. government, and the global economy. Due to the increased speed and efficiency of cyber systems and networks, military supply and logistics chains have been automated; government emergency services rely increasingly on electronic processes; and critical business services have migrated to technology that depends on Internet protocol.

These developments have created the potential for a catastrophic cyber incident on a scale comparable to Hurricane Katrina in 2005. As a result of the increasing pervasiveness of cyber and communications technology, many critical pieces of national infrastructure now rely on complex, interconnected cyber systems. An accident, attack, or natural disaster could impact infrastructure that is critical to public safety, national security, or economic security. Such an incident could be devastating to the lives of Americans or to the security of the nation itself. Although the exact type or likelihood of catastrophic cyber incidents is unknown, the consensus is that the potential results of such incidents could be dire. Thus, prevention and preparedness efforts, response procedures, and recovery plans are required.

Unfortunately, the federal government has displayed irresolute and inconsistent leadership regarding cyber critical infrastructure protection. Much of its effort has been directed at general “outreach” and “awareness” activities, rather than at developing robust and comprehensive prevention, response, and reconstitution programs for attacks against critical cyber systems. Federal policy has neither clearly defined factors that would comprise a Cyber Incident of National Significance, nor specified triggers and thresholds for action during an emergency. Vague policies have resulted in little operational guidance for federal response entities if such an event were to occur. The existing guidance does not clearly delineate roles and responsibilities for stakeholders in the federal government, or provide expectations for private-sector entities. In addition, the government has shifted its focus and resources away from issues critical to national security, such as a cyber attack with catastrophic consequences, and toward criminal and consumer protection issues, such as identity theft and data breaches. In this chapter, we give some historical background, detail the reasons for our conclusions, and provide some recommendations.

Background of Critical Infrastructure Protection

During the two world wars, the United States instituted civil defense programs that related directly to the fear of domestic invasion by the nation-state enemy being fought abroad. The focus was primarily on preventing a physical attack by conventional means. Today’s concept of critical infrastructure protection (CIP) similarly reflects the fear of attacks by foreign enemies against domestic assets, but it incorporates threats from native saboteurs and from nature. CIP also integrates a new threat spectrum, which includes attacking through complex cyber systems.

The first major policy document on CIP was the 1997 report of the President’s Commission on Critical Infrastructure Protection (PCCIP).¹ Since then, numerous CIP offices have been established within federal, state, and local governments, as well as within research institutions.

There have also been various laws and regulations relating to CIP. In 1998, Presidential Decision Directive 63 (PDD-63) identified principles for protecting the United States from cascading disruptions that could result from the interdependence of critical infrastructures, and for guarding against attacks on our information technology.² In addition, PDD-63 called for a National Infrastructure Assurance Plan, but such a plan was not created until eight years later, in 2006.³

After the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act. In this legislation, Congress defined critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”⁴

It could be said that the 1997 Report of the PCCIP conceptualized infrastructure protection; PDD-63 in 1998 attempted to implement those concepts; and in 2001 the USA PATRIOT Act codified them. Then, in 2003, President George W. Bush released the National Strategy to Secure Cyberspace, and in the same year issued Homeland Security Presidential Directive 7 (HSPD-7), which mandated the development of a national CIP plan as PDD-63 had requested five years earlier.⁵

In the meantime, cyber issues were again rising to the forefront among policymakers. In 2005, the leadership of the Department of Homeland Security (DHS) cyber office, formerly a position at the Division Director level, was elevated to Assistant Secretary for Cyber and Telecommunications Security. This position was filled late in 2006.

Responding to the HSPD-7 mandate, the Department of Homeland Security finalized its National Infrastructure Protection Plan (NIPP) in 2006.⁶ The NIPP is meant to be a comprehensive risk management framework for the protection of U.S. infrastructure. However, the early drafts of the plan did not do much to address cyber issues. While cyber concerns were incorporated in the final NIPP, the document lacks specific guidance as to how to integrate physical and cyber protection plans.

The U.S. government’s critical infrastructure efforts span many different aspects of the threats and vulnerabilities facing the nation. The question of what specific assets and processes comprise critical infrastructure is itself the subject of intense debate; a thorough examination of all aspects of critical infrastructure is not attempted here. Rather, this chapter reviews stakeholder efforts to protect cyber and communications infrastructure, pressing cyber CIP concerns, and shortfalls in adequately addressing those concerns.

Importance of Cyber CIP

Paraphrasing the 2003 National Strategy to Secure Cyberspace, DHS has described cyberspace as “the nervous system of the Nation’s critical infrastructures, the control system of our country and the global economy.”⁷ Congress has explicitly recognized the role of information technologies (IT), noting that “[p]rivate business, government, and the national security apparatus increasingly *depend on an interdependent network of critical physical and information infrastructures*, including telecommunications, energy, financial services, water, and transportation sectors.”⁸

Cyber CIP and Government Emergency Response

The cyber infrastructure plays a large role in the government’s emergency response capabilities, serving as an enabler in critical processes and procedures. Organizations and personnel responsible for the health and safety of citizens rely on cyber technology at almost every turn. As the Business Roundtable emphasized in a report on cyber preparedness, first responders use the IT infrastructure to coordinate and manage responses to catastrophic events, including dispatching emergency personnel, communicating with law enforcement, health, and fire professionals, and tracking essential supplies via the Global Positioning System.⁹ Thus, protection of the cyber infrastructure is essential to emergency response capabilities.

The role of cyber infrastructure in emergency response is also critical to areas such as transportation of supplies and personnel, government communication with the populace, and the restoration of public confidence during an emergency. The cyber infrastructure is an integral part of the nation’s communications infrastructure, due in part to the convergence of communications and cyber capabilities and infrastructure. If the cyber infrastructure that supports communications capabilities were to fail, there would be a large impact on the government’s ability to warn and inform citizens during an emergency. The government’s ability to coordinate messages and information among multiple emergency response entities would also be affected. The lack of coordinated information and guidance from the government harms public confidence and could possibly cause physical danger to citizens, as illustrated by the problematic evacuation processes during Hurricane Katrina in 2005.

Another vital part of the government's emergency response structure is its ability to move supplies and personnel through areas quickly and efficiently. Areas in crisis need everything from medical supplies and food, to engineers and computer experts. The federal government's report on lessons learned after Hurricane Katrina highlighted the fact that resource managers did not have a clear idea of what was needed and what was available, due to poor management of assets and logistics. The government's supply chain was highly bureaucratic and outdated.¹⁰ Cyber CIP has a major role in the systems and networks used to update and modernize the government's supply-chain capabilities. If advanced cyber security solutions are not integrated as core processes within these updated and modernized supply networks, we will simply be increasing the quantity and dependency of such vital systems, and thus enhancing their vulnerability.

Cyber CIP and the Military

The U.S. military is one part of the federal government that does possess a well-developed and modernized supply chain and logistics system. In order to be able to carry out its mission of protecting the United States, the Department of Defense (DOD) needs to be able to transport large amounts of matériel and personnel quickly, safely, and efficiently. It operates a massive supply-chain system that stretches around the world. Cyber capabilities play a large role in operating and maintaining this structure, making cyber CIP a critical component of DOD's warfighting capability.

Technology also supports other important DOD functions in addition to supply and logistics. It is a vital part of many of the military's weapons systems, directly supporting warfighting capability. Everything from tanks and missiles to fighter planes and ships rely on cyber technology. Accordingly, the military has recognized the importance of this aspect of its fighting capability and has taken some steps to protect its vulnerable systems and assets.

In regard to the protection and defense of cyber systems and data, DOD has formulated clear policy, constructed operational structures, and acquired the technological capabilities to protect its systems. DOD policy requires strict oversight of cyber security, including asset identification and management. Formal procedures delineate roles and responsibilities and provide guidance on how to implement policy. The military not only purchases significant amounts of information security technology, it also integrates information security into the entire asset life-cycle process for all purchases.¹¹ The DOD model could be leveraged by other governmental entities seeking to improve security for cyber assets.

Recognizing that both the threats against its systems and information and their vulnerabilities are growing daily, the military is conducting research and development, operations, and exercises to test its weaknesses and enhance its capabilities. DOD has taken a proactive approach to addressing cyber issues that should be adopted by other organizations, both public and private, that have significant responsibilities for protecting critical cyber systems. Given the role that technology plays in DOD's mission to defend the security of the nation, the military is attempting to address the risks associated with its cyber reliance. However, there are other major aspects of national security that the military does not control.

Cyber CIP in the National and Global Economy

The danger from threats to cyber and communications infrastructure is not limited to lives and physical infrastructure. The nation's economy is a crucial piece of the national security landscape. Financial markets are very dependent upon cyber technology, and this reliance can cause cascading problems.

For example, a massive sell-off of stocks occurred on one day in February of 2007. The extraordinary trading volume carried its own inherent problems, but several cyber incidents exacerbated these problems. A computer glitch caused a time lag of more than an hour in calculating the value of the Dow Jones Industrial Average. When calculating operations were shifted to a backup computer, prices suddenly caught up and were processed all at once, and as a result there appeared to be an immediate 200-point drop in the Dow Jones average. With all this confusion, the Dow suffered its biggest drop since the first trading day after the terrorist attacks of September 11, 2001.¹²

In addition to the Dow Jones computer problems, intermittent systems problems and communications delays occurred at the NASDAQ, American Stock Exchange, and New York Stock Exchange, and numerous online brokerage companies suffered slowdowns in their networks. For a time that day, it was estimated that one out of four online stock transactions could not be completed.¹³

There are technological and human safeguards in place to prevent such glitches from becoming uncontrolled and wreaking havoc on the markets, but these measures are not infallible. Plans should be in place not only for protection, but also for response and reconstitution of all assets, including public trust.

Some experts question whether the U.S. National Response Plan (NRP), to be utilized after natural disasters and terrorist attacks, is relevant to cyber incidents that cause market harm. Public trust is a huge factor in any response to a damaged financial system. Any cyber incident that results in Internet disruptions could also have a major impact on financial markets. Thus, for cyber incidents, some experts have called for a national response mechanism that balances traditional first-responder priorities of the NRP with market and public trust priorities.¹⁴

In addition to its role in the U.S. economy, cyber infrastructure plays a major role in trade and financial services in markets and economies around the world. A major cyber incident could have impacts similar to or worse than the Dow Jones glitch of February 2007. The global system of finance is now so interconnected that actions and events in one market or location often result in widespread ripple effects.

As new connections are established and new stakeholders join daily, the global system becomes more and more complex, thereby increasing the chances that the impact of an incident could ripple into the U.S. economy from an unexpected source. The critical cyber infrastructure that helps operate the financial networks and systems in countries outside of the United States can still have impacts on U.S. economic security. These effects, and the behavior of the whole global economic system, are not receiving adequate attention from the policymakers dealing with cyber CIP. The United States and its financial partners should intensify efforts to understand the interconnections and the cyber vulnerabilities of the global economy, and should include both market effects and public trust impacts in future response plans and guidance.

Potential for Catastrophic Cyber Incidents

An accident, a natural disaster, or an attack on elements of critical infrastructure that depend on cyber technologies could have Hurricane Katrina-level results. Damage could be caused by disruption of cyber systems or by weaponization of the cyber infrastructure. Disruption could result from either a natural disaster or a manmade situation. There is no agreement on the probability of, or timeframe for, such an incident, or on what a cyber catastrophe would look like.¹⁵ There is no doubt, however, that such an incident is possible due to the vulnerabilities inherent in the hardware and software critical to the Internet, and the threats facing the nation's cyber infrastructure.

Despite its resiliency, significant vulnerabilities exist in the infrastructure of the Internet. Attacks on the 13 root servers, submarine cables, or telecommunications hotels could

affect significant portions of the Internet. There are also vulnerabilities in the software supporting Domain Name System servers that permit Internet traffic to flow. These vulnerabilities present many different opportunities to those looking to damage the United States. The range of threats confronting the safety and security of America includes threats from organized nation-states as well as various terrorist groups. Security experts are aware that the plans of attack of particular nation-states include strikes on cyber infrastructure.¹⁶ There are also indications that terrorist groups such as Al Qaeda are considering cyber-based attacks on electrical grids and financial institutions.¹⁷

An attack on cyber infrastructure that has consequences at the national level moved beyond abstract possibility in the spring of 2007. The small Baltic country of Estonia experienced “massive and coordinated cyber attacks on Web sites of the government, banks, telecommunications companies, Internet service providers and news organizations.”¹⁸ Like most countries, Estonia relies heavily on its cyber infrastructure, and the attacks did serious damage — from the crashing of government computers that had to be taken offline, to the disabling of payment systems, which prevented citizens from making non-cash purchases.¹⁹

If similar attacks were to take place in the United States, damage could be extensive. Attacks or incidents could impact public safety (for example, an attack on the control systems of a dam to facilitate the sudden and unexpected flooding of a downstream city); national security (such as an attack that gained access to U.S. intelligence or military information); or economic security (such as a misinformation and systems attack that undermined confidence in the integrity of U.S. financial networks). Each type of attack is addressed in turn here.

Public Safety

More than ever, the public’s health and welfare are dependent on cyber infrastructure. In addition to the major role cyber technology plays in the missions of first responders, it is also vital to operating and maintaining critical infrastructure on which the physical safety of thousands of people may depend. For example, a cyber incident or attack affecting the systems that control nuclear facilities or dams could be devastating if it resulted in the flooding of a city downstream from a dam, or an explosion that spread radiation over a wide radius.

Supervisory Control and Data Acquisition (SCADA) systems, or process control systems, control the operations of many different critical infrastructures, such as power plants, chemical and nuclear facilities, oil and gas pipelines, and water treatment plants. In the past, several SCADA attacks have posed direct threats to health and safety, including a 1997 attack in Worcester, Massachusetts, that disabled a telephone network that served fire departments, an airport, and local residents.²⁰ The “Slammer” worm of 2003 disabled a safety monitoring system at a nuclear power plant and blocked control-system traffic at five other utilities.²¹ Although the attacks on SCADA systems so far have not caused catastrophic damage, they demonstrate the vulnerability of systems that affect the safety and health of thousands of people. Larger and more determined attacks, such as those inflicted upon Estonia, could do far more damage.

National Security

Also included in the realm of cyber CIP are federal systems that contain sensitive information. These systems may contain data critical to national security, such as military capabilities and foreign intelligence. If such information were compromised, the effects might damage the military’s ability to protect the nation, or the government’s ability to detect threats.

There have been many attempts to probe the cyber defenses of the government; for example, a series of attacks have targeted federal agencies ranging from the DOD to the National Aeronautics and Space Administration.²² Departments possessing highly sensitive information have experienced data breaches and hacks. State Department networks were breached in June 2006, resulting in a potential loss of information, as well as a chance that the perpetrators had opened hidden, backdoor paths of attack into the system.²³

These attacks have been significant, but they are largely discrete and separate attacks. No massive, coordinated effort to take down military, intelligence, and diplomatic systems has yet been identified. However, judging by the damage caused by the individual attacks that have occurred to date, an attack on the scale of the Estonia campaign could have serious ramifications for national security. An attack of this nature could reveal the potentially large gaps in U.S. policy and doctrine about how the nation would respond to cyber attacks.

Economic Security

In the event of an attack, public confidence in U.S. financial and monetary stability could be harmed in the absence of adequate guidance and reassurance from the government. If citizens are not assured that their money is safe and available, the economic effects could be severe. The financial and economic system relies on the trust of its citizens as well as international stakeholders. The government has a responsibility to communicate situational and other information in such a way that incidents will not needlessly damage national or global financial institutions.

Given the vital role that cyber technology plays in national and international economic systems, an attack on Internet hardware or software could also have a major impact on the global economy. The ripple effects of the Dow Jones computer glitch described above affected other exchanges at the national level, and subsequent drops in value affected stock exchanges abroad. Although this glitch was not an intentional attack, it had global consequences. An intentional and targeted attack, building on the lessons learned from the Dow Jones incident, could be far more detrimental to the international system of trade and finance.

The danger from cyber attacks or accidents comes not just from incidents originating in financial systems abroad or within domestic stock exchanges. Due to the convergence of cyber technology, many of the businesses that comprise the U.S. economy utilize the same cyber and communications infrastructure. The interconnection of systems brings many benefits, including improved efficiency, speed, and capability. However, the technology that underpins these capabilities may contain vulnerabilities that can be exploited.

Not only do businesses rely on the same technology for critical business functions, they also rely on *other* businesses and sectors. Any attack or incident that caused a major failure in a critical infrastructure, such as the power or telecommunications sectors, could affect other businesses and sectors nation wide. Thus, a single business can have multiple key dependencies and interdependencies, and it might not even be aware of all of them. Understandably then, the extent of cyber and communications dependencies across one sector of the economy, much less those dependencies across the nation, can be difficult to comprehend. A disruption within any cyber or communications technology that supports businesses could ripple up from the individual business and sector level to affect the national economy.

Federal Leadership

Although the private sector will lead the efforts to develop solutions to cyber and communications infrastructure vulnerabilities, it is the government that must lead efforts in the preparedness for, response to, and recovery from catastrophic incidents. This is the first time that the private sector has had such a large role in protecting national security, and the first time that it has been asked to shoulder such a large burden. In the case of cyber and communications CIP, the federal government must rely extensively on the private sector. However, it cannot delegate its inherently governmental responsibility for the protection of life and property.

The best way forward is for the government to serve as an organizational model, to develop and test emergency practices, and subsequently bring its expertise to the private sector to be leveraged as best practices. For the federal government to guide the private sector, however, it will need to provide clear policy direction, develop operational guidance that specifies roles and responsibilities, and shift its research and development priorities and its distribution of resources to the task of preventing and managing catastrophes. The federal government must lead by example, by offering an effective model for preparedness, response, and recovery. However, its efforts to date have fallen short.

Misdirected and Ambiguous Federal Policy

Federal leadership is crucial to cyber-related CIP issues because cyber threats and incidents will rarely be limited to local or state effects. The 2003 National Strategy to Secure Cyberspace specifies that the federal government is responsible for such cyber issues as “forensics and attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against organized attacks capable of inflicting debilitating damage to the economy.”²⁴

However, cyber issues have suffered from a lack of consistent leadership from the federal government. Despite language in the USA PATRIOT Act that emphasizes “virtual” as well as physical systems and assets, the federal spotlight has been on the protection of the latter. Cyber-related CIP issues have not received focused or consistent attention. In its first major policy document, DHS took steps toward developing a national plan for CIP: it issued the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, but, as its title indicated, this document focused on physical assets, not cyber assets or protection against cyber threats.

The strategic objectives of the 2003 National Strategy to Secure Cyberspace are to prevent cyber attacks against critical infrastructures, reduce national vulnerability to cyber attacks, and mitigate against damage and improve recovery time from cyber attacks.²⁵ However, the primary focus of DHS is still on “awareness” — spreading the word that cyber security is an important concern. In a speech in early 2007, the new DHS Assistant Secretary for Cyber and Telecommunications Security encouraged the private sector to perform vulnerability assessments and implement security policies.²⁶ Such advice and awareness are inarguably important, but fail to differentiate between the majority of everyday security issues which are not critical, and the security of those systems and assets that, in the words of the USA Patriot Act, are “so vital to the United States that [their] incapacity or destruction ... would have a debilitating impact on security, national economic security, national public health or safety.” The policy and operational issues regarding the security of such vital systems or assets must be examined.

One example is the federal authority to declare an Incident of National Significance. The NRP Cyber Annex states that “[c]yberspace is largely owned and operated by the private sector; therefore, the authority of the federal Government to exert control over activities in cyberspace is limited.”²⁷ Since no new laws have been passed regarding authorities during a cyber incident, the extent of federal power during such an incident has not been openly delineated. An analysis of the extent of federal authority in such circumstances would encompass not only disaster response authorities but also federal powers under the Defense Production Act, such as setting priorities for access to cyber assets and for reconstitution.²⁸ There is no clear sign that the federal government has yet undertaken such an analysis.

Moreover, the phrase “Cyber Incident of *National Significance*” may be anomalous because, although an incident may have a national effect, a catastrophic cyber incident would likely be global in nature. Here, too, the federal government has not yet provided leadership on international cyber response and recovery issues.

The government must provide a clear definition of the factors that determine a Cyber Incident of National Significance, including specific triggers and protocols for response escalation. This policy should clarify the legal authorities of the federal government during a cyber incident, and set goals for expected federal interactions with the private sector and with government entities at the state and local level. It should strengthen international understanding of and cooperation on cyber issues, and establish initiatives to engage the international community in discussion of appropriate actions during cyber crises.

The federal government should also set expectations for the private sector. The business community plays a major role in critical infrastructure protection, but there is widespread confusion as to how it should prepare for, respond to, or recover from catastrophic cyber incidents. The private sector owns and operates a large share of the critical infrastructure in the United States, but the federal government, too, owns and operates much of it. As part of its traditional role of managing catastrophic incidents, the government has a responsibility to protect this infrastructure. The U.S. government should leverage its extensive global networks to establish early warning and information sharing protocols that could be used by both the government and private sector in the event of emergency.

In serving as a leader to the private sector, the federal government should inform the private sector of what it can expect from government departments and agencies; establish minimum expectations for actions from the private sector; and mandate liabilities for failure to perform in a satisfactory manner. It should also establish central points of contact that are easily accessible to private-sector stakeholders. These government actions to manage catastrophic incidents should be clearly defined, so as to provide clear guidelines to the private sector.

The private sector also has a responsibility to protect its infrastructure. The business community must take the initiative and not simply wait for guidance from the federal government. Private-sector stakeholders must join to form their own points of contact. The Information Sharing and Analysis Centers (ISACs) now established in several critical industry sectors are a start, but more is needed. The private sector should communicate with the government and establish joint expectations that are acceptable to both the public and private sectors. Business leaders should focus efforts on learning how to manage important economic issues that may be affected by a cyber disruption, such as public trust and confidence in the markets.²⁹ CEOs and other senior business officials must plan within their own companies and industries in order to maintain business functionality during catastrophic incidents.

Lack of Federal Operational Guidance

While some federal policy documents have recognized the importance of cyber CIP issues, there has been little government follow-through or implementation. High-level policy discussion has been lacking within DHS to formulate specific plans and guidance for dealing with cyber catastrophes. The National Infrastructure Protection Plan contains cyber language at the strategic level, but does not address the operational level. Similarly, the Cyber Annex to the National Response Plan contains little specific guidance. As of

early 2007, DHS was still working “to refine written documentation establishing a concept of operations” for how federal departments and organizations and the private sector would work together during a cyber incident.³⁰ Further, although the NRP states that the administration has the authority to declare a Cyber Incident of National Significance, it does not specify the factors that indicate what would constitute such an incident, nor has DHS spelled these out. The departments and agencies of the federal government do not currently have plans for how to respond if such an incident were declared, nor do they have a unified plan for how to coordinate their response with other agencies, state and local level government, the private sector, or international organizations.

The federal government must move forward to generate operational guidance. In particular, it must delineate the roles and responsibilities of DOD and other federal entities for emergency response to a cyber incident. These roles and responsibilities should be based on an escalating scale of triggers and thresholds that are clearly set forth in policy that includes definitions of emergencies and missions, and identification of essential personnel. Across two administrations, presidents have signed national strategies mandating results in this area, but cyber remains one of the least-developed areas of homeland security policy. This must change.

Allocation of Resources

As the Cold War ended, a new and complex set of challenges arose, and U.S. leaders realized that priorities and assets at the national level would have to be reoriented. However, in the cyber realm, the government has shifted its priorities and resources away from national security issues such as preparing for a catastrophic cyber incident, instead focusing funding on cyber crime, identity theft, and consumer protection issues.

DHS seems to spend more time on “outreach” and “awareness” activities than on identification of critical assets and critical infrastructure protection issues. This imbalance reflects Congressional appropriations. For fiscal year 2007, Congress appropriated as much for “Critical Infrastructure Outreach and Partnership” within DHS (\$101.1 million) as it did for both critical infrastructure “Identification and Evaluation” and “Protective Actions” combined.³¹ By these numbers, Congress gave “outreach” the same funding priority as actual protection.

While recognizing these external mandates, DHS's internal allocation of its cyber security budget could still improve to address what is truly critical in a meaningful and efficient manner. For example, in 2005 the National Cyber Security Division (NCSD) at DHS spent \$15 million on a SCADA security program.³² But NCSD also spent \$3 million, or one-fifth as much, on a single four-day tabletop exercise called Cyber Storm.³³ It may be questioned whether one four-day exercise was worth one-fifth of a year's expense for a program to improve control system security. The value of Cyber Storm may be further cast into doubt when one considers its purpose and major findings. One main goal was to exercise the established response policies, procedures, and communication mechanisms during a cyber crisis. However, as already discussed, there are no clear, formal operating procedures for federal cyber incident response. Thus, it should not be surprising that one conclusion from Cyber Storm was that we need clearly defined, well thought-out, formalized response plans for such contingencies.³⁴ It is unclear, however, why DHS apparently needed to spend \$3 million to reach that conclusion.

Positive Steps

While the federal government has not provided consistent leadership in cyber issues in the past, there is still hope that we may be moving onto the right path. In February of 2007, nearly a decade after the President's Commission on Critical Infrastructure Protection, DHS announced that it would be collocating its watch and warning personnel at the U.S. Computer Emergency Readiness Team with private-sector warning teams from the Communications ISAC. DHS also expects to collocate government staff with private-sector staff from the Information Technology ISAC warning teams, with the goal of establishing a "collaborative, real time and trusted information sharing environment that enables us to see what's happening on our networks and take immediate steps to fend off attacks."³⁵ DHS eventually expects to strengthen this capability with other sectoral ISACs, to give a "synthesized, cross-sectoral view and incident response capability."³⁶ Although there have been delays in arriving at these steps, such programs are encouraging.

Conclusion and Recommendations

The federal government must now move beyond a focus on “awareness” to identify what is truly “critical” in cyber CIP: an incident that could create a catastrophic result in terms of physical or economic harm. That which is critical to a state or locality needs only a commensurate level of preparedness and response. That which is critical to the nation ,or to the global economy and communications systems, needs a much greater level of preparedness and response.

The federal government must, therefore, overhaul its current position and do better at preparing for cyber incidents, update its approach to partnering with the private sector, and shift resources towards emergencies at the national and global levels. It must embrace its role and responsibility to lead preparedness and response efforts for catastrophic cyber and communications incidents. It should start by establishing policy that clearly defines what constitutes a Cyber Incident of National Significance, and follow it with operational guidance that outlines federal roles and responsibilities during such an incident. Guidance should also include a set of expectations for the private sector and international stakeholders. The federal government should establish a system for response to economic and market disruption resulting from a cyber incident.³⁷ And it would also be helpful to develop federal operational guidance to implement existing strategic policy, and engage global stakeholders.

Cyber and communications critical infrastructure protection plays a crucial role in the nation’s economic and national security, as well as the critical functions that the government provides. These technologies are embedded in processes that are vital to the nation and its citizens — from the processes that operate the financial markets, to the systems that run tanks and planes, to the devices used by first responders. The new and ever-expanding role of such cyber systems, combined with their inherent vulnerabilities, has resulted in the potential for a catastrophic cyber incident. Interdependencies and the pervasive nature of cyber infrastructure mean that unexpected cascading effects can undermine these vital processes. The possibility of such an incident grows greater as cyber and communications technologies are increasingly interwoven into national and economic security, as well as core emergency response functions. The federal government can, and must, do better at protecting the critical cyber infrastructure of the United States.

NOTES

¹ President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: U.S. Government Printing Office, 1997), available at http://permanent.access.gpo.gov/lps15260/PCCIP_Report.pdf.

² Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," May 22, 1998, available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

³ Department of Homeland Security, *National Infrastructure Protection Plan* (2006), available from http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

⁴ "USA PATRIOT" Act, Pub. L. No. 107-56, § 1016(e) (2001) (prior to 2006 reauthorization).

⁵ White House, National Strategy to Secure Cyberspace (February 2003), available at <http://www.whitehouse.gov/pcipb/>; Homeland Security Presidential Directive 7 (HSPD-7), December 17, 2003, available at <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>.

⁶ The National Infrastructure Protection Plan (NIPP) is described at and can be downloaded from http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

⁷ Department of Homeland Security, *Information Technology Sector Overview, National Infrastructure Protection Plan*, http://www.dhs.gov/xlibrary/assets/nipp_it.pdf (last accessed June 18, 2007).

⁸ USA PATRIOT Act, § 1016(b)(2). Emphasis added.

⁹ Business Roundtable, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness: New Priorities and Commitments from Business Roundtable's Security Task Force 4* (2006), <http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf>.

¹⁰ White House, *The Federal Government's Response to Hurricane Katrina: Lessons Learned* (February 2006), p. 56.

¹¹ See DOD Directive 8500.01E; Department of Defense Instruction, Information Assurance (IA) Implementation, No. 8500.2 (February 6, 2003).

¹² Keith Regan, "Computer Glitches Heaped Fuel on Stock Sell-Off," *E-Commerce Times*, March 1, 2007, <http://www.ecommercetimes.com/story/56032.html>; Jessica Dickler, "Technical Glitches Plague Wall Street," *CNNMoney.com*, February 27, 2007, http://money.cnn.com/2007/02/27/markets/dow_drop/index.htm; Thomas S. Mulligan, "A Computer Glitch Distorts Dow's Drop, Then Exacerbates It," *Global Technology Forum*, February 28, 2007, http://ebusinessforum.com/index.asp?layout=rich_story&doc_id=10212; Associated Press, "Computer Glitch Triggered Dow Jones Plunge," February 27, 2007, available at <http://www.kstp.com/article/stories/S33513.shtml?cat=1>.

¹³ Mulligan, "A Computer Glitch Distorts Dow's Drop, Then Exacerbates It."

¹⁴ Business Roundtable, *Essential Steps to Strengthen America's Cyber-Terrorism Awareness*, p. 14.

-
- ¹⁵ See Chapter 7 in this volume, “Information Security Issues in Cyberspace” by Ed Skoudis.
- ¹⁶ See, e.g., Century Foundation Task Force, *The Forgotten Homeland* (New York: Century Foundation Press, 2006), pp. 112–113.
- ¹⁷ Justin Blum, “Hackers Target U.S. Power Grid,” *Washington Post*, March 11, 2005, p. E1; Agence France-Presse, “Police Foil al-Qaida Net Attack,” March 12, 2007, available at <<http://australianit.news.com.au/story/0,24897,21365277-26199,00.html>>; David Leppard, “Al-Qaeda Plot to Bring Down UK Internet,” *Times Online*, March 11, 2007, <<http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece>>.
- ¹⁸ Peter Finn, “Cyber Assaults on Estonia Typify a New Battle Tactic,” *Washington Post*, May 19, 2007, p. A1.
- ¹⁹ Larry Greenemeier, “Estonian Attacks Raise Concern Over Cyber ‘Nuclear Winter,’” *InformationWeek*, May 24, 2007, available at <<http://www.informationweek.com/news/showArticle.jhtml?articleID=199701774>>; Jaikumar Vijayan, “Hackers Evaluate Estonia Attacks,” *Computerworld*, August 4, 2007, available at <<http://www.pcworld.com/article/id,135503-page,1/article.html>>.
- ²⁰ Cyber Security Industry Alliance, “SCADA: Get the Facts,” April 2007, pp. 3–4, <https://www.csialliance.org/publications/csia_whitepapers/CSIA_SCADA_Get_Facts_April_2007.pdf>.
- ²¹ *Ibid.*
- ²² “Addressing the Nation’s Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action,” Hearing Before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology of the House Committee on Homeland Security, 110th Cong. (2007), pp. 1–2, prepared statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies.
- ²³ Daily Press Briefing by Sean McCormack, Spokesman, U.S. Department of State (July 12, 2006), <<http://www.state.gov/r/pa/prs/dpb/2006/68924.htm>>.
- ²⁴ National Strategy to Secure Cyberspace (February 2003), p. ix (executive summary).
- ²⁵ *Ibid.*, p. viii (executive summary).
- ²⁶ Gregory Garcia, Assistant Secretary for Cyber Security and Communications, U.S. Department of Homeland Security, “Remarks at the RSA Conference on IT and Communications Security” (February 8, 2007), <http://www.dhs.gov/xnews/speeches/sp_1171386545551.shtm>.
- ²⁷ Department of Homeland Security, *National Response Plan*, Cyber Incident Annex CYB-5 (2006), available from <http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm>.
- ²⁸ 50 USC App. § 2061 et seq.; see also Lee M. Zeichner, “Use of the Defense Production Act of 1950 for Critical Infrastructure Protection,” *Security in the Information Age: New Challenges, New Strategies*. Joint Economic Committee, U.S. Congress (May 2002) p. 74-88, available at <<http://www.house.gov/jec/security.pdf>>.

²⁹ Business Roundtable, *Essential Steps to Strengthen America's Cyber-Terrorism Awareness*, p. 2.

³⁰ Garcia, "Remarks at RSA Conference."

³¹ H.R. Rep. No. 109-699, p. 158 (2006) (\$69,000,000 and \$32,043,000, respectively).

³² Caron Carlson and Paul F. Roberts, "DHS Progress Proves Elusive," *eWeek*, September 12, 2005, <<http://www.eweek.com/article2/0,1895,1858740,00.asp>>.

³³ Wade-Hahn Chan, "Cyber Storm Finds Weaknesses," *FCW.com*, October 2, 2006, <<http://www.fcw.com/article96277-10-02-06-Print>>.

³⁴ *See generally*, Department of Homeland Security, National Cyber Security Division, "Cyber Storm Exercise Report" (September 12, 2006), <http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf>.

³⁵ Garcia, "Remarks at RSA Conference."

³⁶ *Ibid.*

³⁷ "[T]he public and private sectors must have a single plan for shoring up the financial markets and public trust and confidence following an event." Business Roundtable, *Essential Steps to Strengthen America's Cyber-Terrorism Awareness*, 16.