

9. CYBER SECURITY A SILENT CATASTROPHE

Cyber attacks occur every day and we easily grow inured to them; it is easy to overlook the fact that our digitally driven economy can be paralyzed by a well planned and executed cyber attack. Today cyber security and contingency planning for cyber attacks is overshadowed by a necessary preoccupation with planning for terrorist assaults involving conventional explosives or weapons of mass destruction. It is a grave mistake, however, to ignore the security and reliability of the information infrastructure. The security of cyberspace is essential to national security and to the economy because financial services, communications, transportation, energy, and the military sectors rely entirely upon cyberspace-based systems without which they could not function.

As with physical attacks, protection, prevention, and recovery from a cyber attack requires careful planning and coordination. The major difference between a physical attack and a cyber attack is that in the case of a cyber attack, there are no citizens or first responders to assist with the crisis. Protection, response, and recovery will primarily be in the hands of technical specialists, including security and networking engineers from technology providers and owners and operators of infrastructure. The role of the federal government is to ensure that these private actors have the necessary capabilities and can deliver a coordinated response.

Standards setting, planning, and coordination between sectors must be led by the federal government. Today, however, little federal leadership exists in the area of cyber security and the talk of “partnership” with the private sector is largely rhetoric. While the policies of the Clinton and Bush administrations have explicitly rejected federal regulation to achieve cyber security, Congress has repeatedly enacted laws that resulted in cyber security regulation for specific sectors. Despite this schizophrenic federal attitude toward regulation, or perhaps because of it, there has been no clearly articulated set of cyber security standards.

Cyber vulnerabilities are ubiquitous in both government and the private sector. Cyber security is an instance of both market and regulatory failure.

As the information infrastructure becomes increasingly complex, the path to a more stable, secure, and resilient information infrastructure must be facilitated by the federal government with strong, concise leadership.

The administration must move swiftly to establish a national information assurance policy, with a clear set of priorities:

- ◆ clarify federal agency roles and responsibilities during a crisis;
- ◆ clearly differentiate overlapping Department of Homeland Security (DHS) and Department of Defense (DoD) activities;
- ◆ bring clarity and consistency to federal regulation of cyber security across the different sectors;
- ◆ build a rapid response and recovery capability; and
- ◆ initiate a concerted research and development effort to develop and deploy resilient networks.

In this chapter, we will review the threat from cyber attacks, discuss the importance of federal leadership for cyber security, lay out the principles that should guide the development of a National Information Assurance Policy, review existing strategies and directives that can inform such a policy, and offer additional detail on the elements of the policy.

THE THREAT

There are two kinds of threat in cyberspace. First, criminals and espionage organizations routinely exploit vulnerabilities in cyberspace to steal identities, extort money, and collect sensitive information. These attacks cost the economy billions and disrupt the lives of millions of Americans. Second, terrorist groups or state actors have the potential to destroy or disrupt essential components of our economy and national security infrastructure via cyber attack. The fact that these attacks have not yet taken place does not mean that they cannot occur. There is a consensus among academic, industry, and intelligence community experts

that such crippling attacks are possible. Indeed, a Chinese military leader openly admitted that China would use such attacks on America in the event of hostilities.¹ The existence of large, new Information Warfare units in the U.S. military suggests that the American government is also readying offensive cyber attack capability. It is not, however, readying commensurate defensive capability to protect the private sector assets upon which the U.S. government and economy rely. We must assume that information systems will be subject to large-scale attack. It is essential that we protect and plan for attacks against information systems alone, and in combination with “traditional” terrorist attacks involving explosives or weapons of mass destruction.

THE IMPORTANCE OF FEDERAL LEADERSHIP

Since the transfer of this issue to the Department of Homeland Security, the importance of cyber security as a federal focus has diminished significantly. Federal research and development (R&D) on cyber security has plummeted. The public-private partnership that had been built to address cyber security challenges has withered. The implementation of the president’s own National Strategy to Secure Cyberspace has returned action on only two recommendations. This administration’s failure to address cyber security is recognized in the private sector and Congress. It reflects the low priority given to the issue by a department dominated by traditional police agencies and focused solely on the threat of incidents that create “body bags.” At the core of this potential disaster exists a lack of understanding of cyberspace at senior levels in the administration, little comprehension of the potential damage from cyber attacks, and an ideological opposition to solutions that involve regulation of cyber security or new federal entities to protect cyberspace. As a result, administration action on cyber security has been limited, slow, and often confined to rhetoric rather than action.

While the private sector has a significant role to play in the protection of critical information infrastructure, DHS is supposed to serve as the nation’s point of coordination for all such efforts. Developing a national information assurance policy requires strong leadership from the federal government, in particular the Department of Homeland

Security. Though the responsibilities of DHS can remain narrowly defined, they are nonetheless significant to U.S. economic and national security. DHS is the focal point for the prevention, response, and recovery from cyber security incidents that can have a debilitating impact on our national and economic security. Senior DHS leadership is needed to build an effective public-private relationship, to understand the technical and global complexities of cyber security, and to marshal the resources necessary to provide an effective partnership with private sector organizations and initiatives. In July 2005, Secretary Chertoff announced the creation of an assistant secretary for cyber security and telecommunications, but to date, the post remains unfilled.

FOUR PRINCIPLES OF CYBER SECURITY POLICY

Before a discussion of current policy and the necessary subsequent steps, readers should understand four basic rules about the security and reliability of the global information infrastructure. These rules should also guide the development of our national information assurance policy.

I. CYBERSPACE IS A TOUGH NEIGHBORHOOD

Significant disruptions occur every day. Two separate backbone providers suffered large-scale outages in fall 2005, one due to an error in router configuration and the other because of cuts in fiber connections at two separate locations. While these were not attacks, restoration of the systems required “powering down” routers and bringing them back online slowly. The speed with which attacks spread is accelerating as they become more sophisticated: In 1999 the Melissa virus took three days to cross the Internet; in 2001 Code Red took only minutes; and in 2003 the SQL Slammer worm spread within seconds. Heading from 2005 into 2006 we saw the first significant “zero day” attack. “Zero day” attacks are significant because they give operators little or no time to react. As a reminder, the 2003 Northeast blackout spread within 43 seconds. This brings new meaning to a “bolt from the blue.”

II. WE MUST EXPECT SOME SERIOUS ATTACKS TO SUCCEED

Despite the best efforts to protect and monitor information networks, ultimately some attacks will disrupt information networks or corrupt data. Cyber attackers face few consequences for their attacks because the probability of being caught or killed is infinitesimal. This presents two important implications. First, we must be prepared to reconstitute networks. Second, we must build networks that can withstand attack or degrade slowly.

III. CYBER ATTACKS ARE DIVERSE AND EVOLVING

Beyond worms, viruses, and denial-of-service attacks, we must also acknowledge more insidious attacks. For example, the slow, quiet manipulation or corruption of financial or health care data (blood types or medication assignments and distribution), or logistics and shipping data, could have a devastating impact; the results could be catastrophic and difficult to untangle. We must also think about reliability and quality of service. Unexplained spot outages in networks will cause a loss of confidence in the availability of information networks. This issue could be particularly vexing as we transition to Voice over Internet Protocol (VOIP) communications.

IV. INFORMATION TECHNOLOGY WILL CONTINUE TO EVOLVE RAPIDLY

The pace of convergence between the public service telephone network and IP networks is accelerating. New technologies such as radio frequency identification tags and nanotechnology are being deployed more widely than ever. In the past year, several cities including Philadelphia, Portland, and New Orleans have announced the deployment of citywide wireless networks to support both citizen and emergency responders.² San Francisco is soliciting bids. Increased reliance will lead to increased vulnerability.

THE EXISTING POLICY FRAMEWORK

Though we lack an overall information assurance policy, three documents provide a framework for federal responsibilities to secure cyberspace: the president's National Strategy to Secure Cyberspace (February 14, 2003); Homeland Security Presidential Directive 7 (HSPD-7, December 17, 2003); and the National Response Plan's Cyber Incident Annex (January 6, 2005).

PRESIDENT'S NATIONAL STRATEGY TO SECURE CYBERSPACE

The president's National Strategy is an appropriate place to start. While its recommendations have received substantial attention, the role envisaged for the federal government is equally important. The president's cover letter for the strategy states:

The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and thereby help to protect the people, economy, and national security of the United States. . . . We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our nation's critical infrastructure and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable and cause the least damage possible.

The strategy adds some additional guidance on the federal role, noting that it is appropriate for the government to assist with forensics, attribute the attack to given perpetrators, protect networks and systems critical to national security, interpret indications and warnings, and protect against organized attacks capable of inflicting debilitating damage to the economy.

Additionally, the strategy holds that the federal government should support research and development that will enable the private sector to secure its critical infrastructure.

The strategy also assigns specific responsibilities to federal agencies, including the Department of Homeland Security. The strategy states that the department should:

- ◆ develop a comprehensive plan to secure critical infrastructure;³
- ◆ provide crisis management and technical assistance to the private sector with respect to recovery plans for failure of critical information systems;
- ◆ coordinate with other federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and non-governmental organizations, including the private sector, academia, and the public; and
- ◆ perform and fund research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

Notably the strategy does not place responsibility for every problem associated with cyber security with DHS, but focuses its role on contingency planning and emergency communications.

HSPD-7

HSPD-7 establishes the U.S. government's policy for the identification and protection of critical infrastructure that, if attacked, would cause catastrophic health effects or mass casualties comparable to a weapon of mass destruction. It advances the president's strategy in a number of areas and helps further refine the federal government's role in securing cyberspace. As discussed previously, HSPD-7 focuses on attacks that would:

- ◆ undermine state and local government capacities to maintain order and to deliver minimum essential public services;
- ◆ damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

- ◆ have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; and
- ◆ undermine the public's morale and confidence in our national economic and political institutions.

HSPD-7 designated the Department of Homeland Security as a focal point for information infrastructure protection, including cyber security, stating: "The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems."

THE NATIONAL RESPONSE PLAN'S CYBER INCIDENT ANNEX

The National Response Plan (NRP) upholds the president's National Strategy to Secure Cyberspace and HSPD-7. The NRP Cyber Incident Annex states that the federal government plays a significant role in managing inter-governmental (federal, state, local, and tribal) and, where appropriate, public-private coordination in response to cyber incidents of national significance.

EXISTING FEDERAL REGULATION

While the policies outlined above explicitly reject federal regulation to achieve cyber security, Congress has enacted laws that resulted in cyber security regulation. Among those laws are:

- ◆ the Federal Information Security Management Act, which regulates security on U.S. government cyber systems;
- ◆ the Banking Modernization Act, which directed eight federal regulatory agencies to establish cyber security standards and audit the agencies to ensure their compliance;
- ◆ the Health Insurance Portability and Accountability Act, which

authorized the Department of Health and Human Services to audit and enforce cyber security standards, although little has been done to implement the law;

- ◆ the Energy Act of 2005, which provides the Federal Energy Regulatory Commission with authority to create cyber security standards for the electrical power grid; and
- ◆ the Sarbanes-Oxley Act of 2002, which resulted in the creation of cyber security standards for publicly traded companies, audited by third-party accounting firms.

BUILDING THE NATIONAL INFORMATION ASSURANCE POLICY

The national information assurance policy would formally establish a framework for protecting the information infrastructure. It would build on the National Strategy to Secure Cyberspace and HSPD-7. The policy would clarify roles and responsibilities and reconcile the number of groups involved in information infrastructure policy setting. It would clearly articulate a set of cyber security standards, developed in conjunction with the nation's experts in the field, and implemented across sectors. It would focus R&D efforts on creating more resilient networks. In support of this directive, an annual report should be prepared for the president's approval, including a requirements-driven multiyear budget, R&D plan, and role and mission statements for all relevant agencies, including the Department of Defense, the FBI, the CIA, the National Security Agency, and the DHS.

DRAWING ON THE EXISTING FRAMEWORK

The president's strategy, HSPD-7, and the National Response Plan yield a possible two-tier framework for federal action.

TIER ONE—FUNCTIONS CRITICAL TO U.S. ECONOMIC AND NATIONAL SECURITY

- ◆ Identify and prioritize critical information infrastructure that, if disrupted, would have a debilitating impact on critical infrastructure or systems essential to U.S. economic or national security.
- ◆ Prepare for such contingencies by ensuring survivable communication networks among key critical information infrastructure operations in the government and private sector.
- ◆ Prepare contingency plans in the event of a disruption that include crisis management and restoration of critical networks, and regularly exercise, test, and refine these plans.
- ◆ Provide for situational awareness and possible warning of attack or disruption to critical infrastructure owners and operators from resources or capabilities that are not available to the private sector, through such means as intelligence.

TIER TWO—FUNCTIONS THAT IMPROVE COORDINATION, AWARENESS, EDUCATION, AND PERSONNEL READINESS

- ◆ Facilitate coordination between individual sectors of the economy by establishing appropriate government advisory committees.
- ◆ Facilitate and support general awareness among all information system users, including home users and small businesses.
- ◆ Track trends and costs associated with information infrastructure attacks and disruptions, through such means as the U.S. Computer Emergency Response Team (U.S.-CERT).
- ◆ Coordinate and support long-term research and development for cyber security.

CLARIFYING ROLES

At least eight agencies and organizations address pieces of the cyber security puzzle. Several have overlapping responsibilities and membership. In

addition, a plethora of committees and commissions are active, including the President’s Homeland Security Advisory Council (PHSAC), the President’s Council on Science and Technology, the National Security Telecommunications Advisory Council (NSTAC), the National Infrastructure Advisory Council (NIAC), the Federal Communications Commission’s (FCC) National Reliability and Interoperability Council (NRIC), the Committee on Foreign Investments in the United States (CFIUS), and the Committee on National Security Systems (CNSS). One committee should be designated for these roles and should reside in the White House.

For operational issues, the directive would seek to clarify DHS and DoD roles in an incident of “national significance.” DHS is responsible for coordinating the response to such an event. However, federal civil capabilities could quickly be overwhelmed, and DoD would be called upon to take a leading role. It is imperative that clear lines of authority be drawn to ensure the federal government can effectively respond to such an incident.

The DoD’s role with regard to indications and warning (I&W) should also be examined. Currently the DoD’s I&W program appears almost exclusively focused on securing its own assets. While this is understandable, it is potentially a crucial mistake, particularly given that privately operated information infrastructure—rather than Defense infrastructure—may be the real target of a terrorist or nation-state attack. The DoD should expand its indications and warning program to include information on potential action against key elements of the private sector, including banking and finance, transportation, energy, and health care. The DoD’s efforts must be fully integrated into a national cyber attack sensing, warning, and response capability.

ENHANCING FEDERAL CAPABILITIES

In order to support this policy, the federal government must build two essential capabilities in conjunction with the private sector:

- ◆ a synoptic, real-time view of the condition of key cyber nodes and systems throughout the United States; and

- ◆ a highly developed and regularly exercised plan to restore secure cyber connectivity, on a prioritized basis, after a significant attack on cyber systems.

To achieve these two capabilities, the federal government will need the following:

- ◆ presidential leadership on cyber security and a presidentially empowered, high-level coordinator;
- ◆ legislative changes concerning public-private partnerships and information sharing and protection;
- ◆ legislative changes to the Wartime Production Act to bring those emergency powers into the information age;
- ◆ increased sentencing guidelines that treat cyber crimes as real crimes and deter would-be hackers; and
- ◆ joint exercises involving the DHS and the DoD, as well as key players in the private sector, should be held to test capabilities and coordination. The DoD should be requested to develop contingency plans for all critical assets, not just those that are critical to the DoD.

BUILDING AND SUPPORTING RESILIENT NETWORKS

The U.S. government, in coordination with the private sector, must accelerate the development of more resilient information networks and systems. Critical elements of the information infrastructure must be resilient and have the ability to degrade gracefully. Ultimately, the United States should strive for self-healing information networks. Of most critical concern are the basic protocols that support the Internet. These include the Domain Name System (DNS), the routing infrastructure, and the current Internet Protocol (IPv4). These protocols are vital to the operation of the Internet, but suffer the “tragedy of the commons” because no entity is responsible for them. An attack

against an obscure but important protocol could cause widespread disruption.

A “secure and reliable” DoD network sitting on top of an inherently vulnerable infrastructure will do little good. DoD should invest money in partnership with DHS and the National Science Foundation to develop new secure networks that will replace today’s Internet. The President’s Information Technology Advisory Committee (PITAC) report, released in 2005, calls for urgent attention to cyber security R&D. The PITAC report lists ten areas requiring additional research, including authentication, monitoring, securing fundamental protocols, holistic system security, mitigation and recovery, and cyber forensics. Unfortunately, the PITAC was allowed to lapse and its work will now be assumed by the President’s Council on Science and Technology. The directive called for above should include R&D and set forth a ten-year plan for developing and deploying secure and reliable information systems.

The vast majority of work in this area rests on research and development. Unfortunately, cyber security has been left by the wayside in terms of federal funding for research and development, and much of DoD’s work in information security remains classified. For example:

- ◆ Defense Advanced Research Projects Agency. The FY 2005 budget for cyber security R&D is \$50 million to \$100 million and is mostly spent on classified projects for DoD.
- ◆ Advanced Research and Development Agency. The FY 2005 budget of \$17 million for cyber security R&D focuses entirely on the intelligence community.
- ◆ Department of Homeland Security. The FY 2005 budget was \$16 million. The budget will likely be cut again and could drop below \$15 million, limiting the capability to continue existing activities. This R&D activity is focused on key aspects of the cyber infrastructure, including DNS, routing, process control systems/SCADA, and national test-beds and test data.
- ◆ National Science Foundation. This agency has the largest piece of the budget for cyber security R&D, at over \$70 million, largely supporting basic research and other grant projects within the higher academic system.

RECOMMENDATIONS

The federal government and the private sector may mistakenly choose to tolerate the rampant criminal activity in cyberspace, but the nation cannot allow a successful terrorist or nation-state cyber attack on essential national capabilities. Nor can the federal government assume that it is necessary to protect only the systems of the Department of Defense. The task force, therefore, highlights the following recommendations:

9.1. A NEW NATIONAL INFORMATION ASSURANCE POLICY SHOULD FORMALLY ESTABLISH A FRAMEWORK FOR PROTECTING CRITICAL CYBER SYSTEMS.

9.2. THE DIRECTIVE SHOULD CLARIFY ROLES AND RESPONSIBILITIES, ELIMINATING OVERLAPPING RESPONSIBILITIES.

9.3. A SINGLE COMMITTEE SHOULD REPLACE THE SIX THAT CURRENTLY ADVISE THE FEDERAL GOVERNMENT ON CYBER SECURITY AND SHOULD RESIDE IN THE WHITE HOUSE.

9.4. THE POSITION OF CYBER CZAR SHOULD BE REINSTATED AND, AMONG OTHER DUTIES, SHOULD HEAD THE COMMITTEE.

9.5. JOINT EXERCISES INVOLVING DHS AND DoD, AS WELL AS KEY PLAYERS IN THE PRIVATE SECTOR, SHOULD BE HELD TO TEST CAPABILITIES AND COORDINATION.

9.6. DoD INDICATIONS AND WARNING EFFORTS MUST BE EXPANDED AND FULLY INTEGRATED INTO A NATIONAL CYBER ATTACK SENSING, WARNING, AND RESPONSE CAPABILITY.

9.7. THE POSITION OF ASSISTANT SECRETARY FOR CYBER SECURITY AND TELECOMMUNICATIONS MUST BE FILLED IMMEDIATELY.

9.8. A CONCERTED EFFORT MUST BE MADE TO DEVELOP AND DEPLOY RESILIENT NETWORKS.

9.9. A SYNOPTIC, REAL-TIME VIEW OF THE CONDITION OF KEY CYBER NODES AND SYSTEMS THROUGHOUT THE UNITED STATES MUST BE DEVELOPED.

9.10. LEGISLATIVE CHANGES CONCERNING PUBIC-PRIVATE PARTNERSHIPS AND INFORMATION SHARING AND PROTECTION SHOULD BE MADE.

9.11. LEGISLATIVE CHANGES TO THE WARTIME PRODUCTION ACT TO BRING THOSE EMERGENCY POWERS INTO THE INFORMATION AGE SHOULD BE MADE.

9.12. INCREASED SENTENCING GUIDELINES THAT TREAT CYBER CRIMES AS REAL CRIMES AND DETER WOULD-BE HACKERS SHOULD BE PUT IN PLACE.

9.13. IN SUPPORT OF THIS DIRECTIVE, AN ANNUAL REPORT SHOULD BE PREPARED FOR THE PRESIDENT FOR HIS APPROVAL, including a requirements-driven multiyear budget, research and development plan, and roles and missions statements for all relevant agencies, including the Department of Defense, the FBI, the CIA, the National Security Agency, and the DHS.

