Securing Cyberspace for the 44th Presidency

A Report of the
CSIS Commission on Cybersecurity for the 44th Presidency

Cochairs:
Representative James R. Langevin
Representative Michael T. McCaul
Scott Charney
Lt. General Harry Raduege, USAF (Ret)

Project Director:
James A. Lewis

Center for Strategic and International Studies
Washington, DC
December 2008

About CSIS

In an era of ever-changing global opportunities and challenges, the Center for Strategic and International Studies (CSIS) provides strategic insights and practical policy solutions to decisionmakers. CSIS conducts research and analysis and develops policy initiatives that look into the future and anticipate change.

Founded by David M. Abshire and Admiral Arleigh Burke at the height of the Cold War, CSIS was dedicated to the simple but urgent goal of finding ways for America to survive as a nation and prosper as a people. Since 1962, CSIS has grown to become one of the world's preeminent public policy institutions.

Today, CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C. More than 220 full-time staff and a large network of affiliated scholars focus their expertise on defense and security; on the world's regions and the unique challenges inherent to them; and on the issues that know no boundary in an increasingly connected world.

Former U.S. senator Sam Nunn became chairman of the CSIS Board of Trustees in 1999, and John J. Hamre has led CSIS as its president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the authors.

1800 K Street, NW
Washington, D.C. 20006
202/775-3175

Contents

Preface

Nearly every day our nation is discovering new threats and attacks against our country's networks. Inadequate cybersecurity and loss of information has inflicted unacceptable damage to U.S. national and economic security. The president of United States must know what these threats are and how to respond to them.

The CSIS Commission on Cybersecurity for the 44th Presidency was established in August 2007 to examine existing plans and strategies and to assess what a new administration should continue, what it should change, and what new policies it should adopt and what new authorities it should seek from Congress. Our report lays out a series of recommendations for a comprehensive national approach to securing cyberspace.

Over the course of our year-long discussions and investigation, the Commission met formally four times; convened more than 30 briefings with government officials and private-sector experts leading the current effort to secure cyberspace; assembled eight working groups; and participated in several congressional hearings and briefings.

We take this opportunity to thank our commission members and working group chairs for their tireless efforts and also the many experts who shared their knowledge and ideas with us. We are deeply grateful to all those who gave generously of their time and insight throughout the project.

James R. Langevin, U.S. Representative
Michael T. McCaul, U.S. Representative
Scott Charney
Lt. General Harry Raduege, USAF (Ret)

Executive Summary

The Center for Strategic and International Studies began this project in August 2007, after the United States suffered a wave of damaging attacks in cyberspace. Guided by our congressional cochairs, we assembled a group of individuals with experience in both government and cybersecurity. The aim of the group was to identify recommendations that the next administration can implement quickly to make a noticeable improvement in the nation's cybersecurity as well as formulate longer-term recommendations that are critical to the nation's future cyber objectives.

The Commission's three major finding are: (1) cybersecurity is now a major national security problem for the United States, (2) decisions and actions must respect privacy and civil liberties, and (3) only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure.

We were encouraged in our work by senior officials in the Department of Defense, the intelligence community, and other agencies who told us that cybersecurity was one of the greatest security challenges the United States faces in a new and more competitive international environment. They encouraged us to think strategically and to be innovative in proposing how the United States organizes itself. Both our findings and their advice are reflected in our recommendations:

Create a comprehensive national security strategy for cyberspace. Comprehensive means using all the tools of U.S. power in a coordinated fashion—international engagement and diplomacy, military doctrine and action, economic policy tools, and the involvement of the intelligence and law enforcement communities. The acronym DIME—diplomatic, intelligence, military, and economic (and with law enforcement a crucial addition)—points to the elements needed for a truly comprehensive solution. This strategy should be based on a public statement by the president that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the United States will protect it, using all instruments of national power, in order to protect national security and public safety, ensure economic prosperity, and assure delivery of critical services to the American public.

Lead from the White House. We used the response to proliferation as a model for how to approach cybersecurity. No single agency is in charge of nonproliferation. Major agencies play key roles set by presidential directives and coordinated by the White House. This is how a comprehensive approach to

cybersecurity must work. We propose creating a new office for cyberspace in the Executive Office of the President. This office would combine existing entities and also work with the National Security Council in managing the many aspects of securing our national networks while protecting privacy and civil liberties. This new office can help begin the work of building an information-age government based on the new, more collaborative organizational models found in business.

Reinvent the public-private partnership. Government must recast its relationship with the private sector as well as redesign the public-private partnership to promote better cybersecurity. A new partnership with more clearly defined responsibilities, an emphasis on building trust among the partners, and a focus on operational activities will result in more progress on cybersecurity.

Regulate cyberspace. Voluntary action is not enough. The United States must assess and prioritize risks and set minimum standards for securing cyberspace in order to ensure that the delivery of critical services in cyberspace continues if the United States is attacked. We advocate a new approach to regulation that avoids both prescriptive mandates, which could add unnecessary costs and stifle innovation, and overreliance on market forces, which are ill-equipped to meet national security and public safety requirements.

Authenticate digital identities. Better authentication significantly improves defensive capabilities. We spent much time constructing a recommendation that emphasized that if privacy and civil liberties are protected, the United States can mandate strong authentication for access to critical infrastructure.

Modernize authorities. U.S. laws for cyberspace are decades old, written for the technologies of a less-connected era. Working with Congress, the next administration should update these laws.

Use acquisitions policy to improve security. The federal government is the largest single customer of information technology products. We recommend that the United States buy only secure products and services; standards and guidelines for secure products should be developed in partnership with industry.

Build capabilities. Research, training, and education will help equip the United States for leadership and security in cyberspace. Because the United States is faced with a plethora of difficult cybersecurity issues, federal support for focused research and development programs will be a critical component of any successful strategy. These efforts will not produce results in the first year, but they will build the long-term capabilities we need for what has become a new domain for international conflict and competition.

Do not start over. The Bush administration took a major step toward improving federal cybersecurity with its Comprehensive National Cybersecurity Initiative. Although the CNCI is not comprehensive and unnecessary secrecy reduced its effect, we believe it is a good place to start. Our Commission shared initial findings with the Bush administration, adjusting them in light of the CNCI's progress, and we have seen them reflected in the CNCI's evolution since the White House announced the formation of the initiative.

In the 1990s, there was considerable discussion of what the international security environment would look like and what the threats to U.S. security would be in that environment. In the past decade, the shape of that new security environment has become clear. Our research and interviews for this report made it clear that we face a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals, and others, and that losing this struggle will wreak serious damage on the economic health and national security of the United States. Finding ways to take better advantage of cyberspace will help give the United States a competitive edge in a world where we are currently running behind, and the ability to operate in cyberspace and to defend against the operations of others will be crucial for our nation to prosper. The United States has begun to take the steps needed to defend and to compete effectively in cyberspace, but there is much to do. The next administration has an opportunity to improve the situation; we hope these recommendations can contribute to that effort.

Summary of Recommendations

Create a Comprehensive National Security Strategy for Cyberspace

1. The president should state as a fundamental principle that cyberspace is a vital asset for the nation and that the United States will protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public.

2. The president should direct the National Security Council (NSC), working with a new office in the Executive Office of the President (EOP)—the National Office for Cyberspace—and other relevant agencies to create a comprehensive national security strategy for cyberspace. Comprehensive means using in a coordinated fashion all the tools of U.S. power—international engagement and diplomacy, military planning and doctrine, economic policy tools, and the work of the intelligence and law enforcement communities.

3. The United States should open the discussion of how best to secure cyberspace and present the issues of deterrence and national strategy to the broad national community of experts and stakeholders.

Organize for Cybersecurity

4. The president should appoint an assistant for cyberspace and establish a Cybersecurity Directorate in the NSC that absorbs existing Homeland Security Council (HSC) functions.

5. A new National Office for Cyberspace (NOC) would support the work of the assistant for cyberspace and the new directorate in the NSC. The president can create this office by merging the existing National Cyber Security Center (NCSC) and the Joint Inter-Agency Cyber Task Force (JIACTF).[1] The assistant to the president for cyberspace would direct the NOC.

6. The NOC, with the new NSC Cybersecurity Directorate and the relevant agencies, would

[1] The JIACTF was created by the director of national intelligence (DNI) to execute DNI responsibilities in monitoring and coordinating the CNCI and to report quarterly to the president on CNCI implementation, together with such recommendations as deemed appropriate.

- Assume expanded authorities, including revised Federal Information Security Management Act (FISMA) authorities, oversight of the Trusted Internet Connections (TIC) initiative, responsibility for the Federal Desktop Core Configuration (FDCC) and acquisitions reform, and the ability to require agencies to submit budget proposals relating to cyberspace to receive its approval prior to submission to OMB;
- Manage both a new federated[2] regulatory approach for critical cyber infrastructures and a collaborative cybersecurity network across the federal government;
- Help develop the national strategy and oversee its day-to-day implementation and the performance of agency elements in securing cyberspace.

7. The president should create three new public-private advisory groups to support the assistant for cyberspace and the NOC.

8. Existing agencies should keep responsibility for their current operational activities, with the Department of Homeland Security (DHS) continuing to be responsible for the United States Computer Emergency Readiness Team (US-CERT), and the US-CERT Einstein program, under the oversight of the NSC and the new EOP cyberspace office. OMB would maintain oversight of the budget functions in coordination (as it does for other policy areas) with the NOC and the NSC.

Partner with the Private Sector

9. The U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities. We recommend the president direct the creation of three new groups for partnership that provide the basis for both trust and action:

   - A presidential advisory committee organized under the Federal Advisory Committee Act (FACA), with senior representatives from the key cyber infrastructures. This new body would incorporate the National Security and Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC);

[2] A federated approach involves individual agencies having some of their actions coordinated by a central authority. Those agencies continue to manage their policies and regulations, but they do so according to a common set of standards developed in a process coordinated by the central authority—in this case, the NOC.

- A town-hall style national stakeholders' organization that provides a platform for education and discussion; and
- A new operational organization, the Center for Cybersecurity Operations (CCSO), where public- and private-sector entities can collaborate and share information on critical cybersecurity in a trusted environment.

Regulate for Cybersecurity

10. The president should task the NOC to work with appropriate regulatory agencies to develop and issue standards and guidance for securing critical cyber infrastructure, which those agencies would then apply in their own regulations.

Secure Industrial Control Systems and SCADA

11. The NOC should work with the appropriate regulatory agencies and with the National Institute of Standards and Technology (NIST) to develop regulations for industrial control systems (ICS). This could include establishing standard certification metrics and enforceable standards. The government could reinforce regulation by making the development of secure control systems an element of any economic stimulus package that invested in infrastructure improvements.

12. The NOC should immediately determine the extent to which government-owned critical infrastructures are secure from cyber attack, and work with the appropriate agencies to secure these infrastructures.

Use Acquisitions Rules to Improve Security

13. The president should direct the NOC and the federal Chief Information Officers Council,[3] working with industry, to develop and implement security guidelines for the procurement of IT products (with software as the first priority).

14. The president should task the National Security Agency (NSA) and NIST, working with international partners, to reform the National Information Assurance Partnership (NIAP).

15. The president should take steps to increase the use of secure Internet protocols. The president should direct OMB and the NOC to develop mandatory requirements for agencies to contract only with

[3] Chief Information Officers Council, http://www.cio.gov/.

telecommunications carriers that use secure Internet protocols. As part of its larger international strategy, the United States should work with like-minded nations and with the ITU and other bodies to expand the use of secure protocols.

Manage Identities

16. The United States should make strong authentication of identity, based on robust in-person proofing and thorough verification of devices, a mandatory requirement for critical cyber infrastructures (ICT, energy, finance, government services). The president should direct the NOC and appropriate agencies, using the federated regulatory model outlined in chapter 4 and consulting with industry and the privacy and civil liberties community, to implement critical infrastructure authentication. The president should receive a report on progress within six months.

17. The United States should allow consumers to use strong government-issued credentials (or commercially issued credentials based on them) for online activities, consistent with protecting privacy and civil liberties.

18. In a related initiative, the Federal Trade Commission (FTC; under its authority under Section 5 of the FTC Act or the Graham-Leach-Bliley Act) should implement regulations that protect consumers by preventing businesses and other services from requiring strong government-issued or commercially issued credentials for all online activities by requiring businesses to adopt a risk-based approach to credentialing.

19. The president should, by the end of the first year of the presidential term, require every agency to report on how many of their employees, contractors, and grantees are using credentials that comply with HSPD-12 (Policy for a Common Identification Standard for Federal Employees and Contractors) and restrict bonuses or awards at agencies that have not fully complied.

Modernize Authorities

20. The president should direct the Department of Justice to reexamine the statutes governing criminal investigations of online crime in order to increase clarity, speed investigations, and better protect privacy.

21. In the interim, the attorney general should issue guidelines as to the circumstances and requirements for the use of law enforcement, military, or intelligence authorities in cyber incidents.

Revise the Federal Information Security Management Act

22. The president should work with Congress to rewrite FISMA to use performance-based measurements of security.

End the Division between Civilian and National Security Systems

23. The president should propose legislation that eliminates the current legal distinction between the technical standards for national security systems and civilian agency systems and that adopts a risk-based approach to federal computer security. The NOC, working with OMB, NIST, and NSA, should develop risk-based standards covering all federal IT systems.

Conduct Training for Cyber Education and Workforce Development

24. The president should direct the NOC to work with the relevant agencies and the Office of Personnel Management to create training programs and career paths for the federal cyber workforce and to work with the National Science Foundation to develop national education programs.

Conduct Research and Development for Cybersecurity

25. The NOC, working with the Office of Science and Technology Policy (OSTP), should provide overall coordination of cybersecurity research and development (R&D). As part of this, the United States should increase its investment in longer-term R&D designed to create a more secure cyber ecosystem.

Introduction
The Hidden Battle

Many people know the story of Ultra and Enigma. Enigma was the German military encryption machine in World War II; Ultra was the British program to crack the German codes. The British, through a combination of skill, luck, and perseverance, were able to collect and decrypt sensitive German military communications and essentially became part of the German military network. This gave them an immense advantage and made allied success more rapid and assured. The outcome of an invisible struggle between Britain and Germany in a precursor to cyberspace gave one side an immense advantage.[4]

The United States is in a similar situation today, but we are not playing the role of the British. Foreign opponents, through a combination of skill, luck, and perseverance, have been able to penetrate poorly protected U.S. computer networks and collect immense quantities of valuable information. Although the most sensitive U.S. military communications remain safe, economic competitors and potential military opponents have easy access to military technology, intellectual property of leading companies, and government data. These potential opponents have not hesitated to avail themselves of the opportunities presented by poor cybersecurity.

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. It is, like Ultra and Enigma, a battle fought mainly in the shadows. It is a battle we are losing.

Cyber attack is a new kind of threat to the safety and well-being of the United States and its allies. In some ways, the story of Ultra and Enigma understates the problem that the United States confronts in cyberspace. The immediate risk lies with the economy. Most companies' business plans involve the use of cyberspace to deliver services, manage supply chains, or interact with customers. Equally important, intellectual property is now stored in digital form, easily accessible to rivals. Weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors. In the new global competition, where economic strength and technological leadership are as important to national power as military force, failing to secure cyberspace puts us at a disadvantage.

[4] This report makes use of a broad definition of cyberspace that goes beyond the Internet to include all forms of networked, digital activities.

For the past 20 years, the United States has struggled unsuccessfully to devise a strategy to counter these new kinds of threats and to protect its interests in a new kind of world. Devising a national strategy has proved to be difficult for many reasons, the most important of which has been that the pace and direction of change in the international environment exceeded our expectations and our ability to predict the direction that change would take. We have not been able to easily discern what threats we would face, what the tools of influence would be, or who would become our opponents. The outcome has been a kind of strategic indecision that puts the United States at risk.

The outlines of the new global strategic environment are becoming clear. It is deeply competitive, although this competition will usually not take the form of traditional superpower confrontation. Cooperation, competition, and conflict, at some level, will be routine elements of the international environment and of our interactions with most other nations. Fleets, armies, and military alliances will not be as important in this competition as the ability for a nation to accelerate its technological progress and economic growth, to create new ideas and products, and to protect its informational advantages. Gaining asymmetric advantage over an opponent will be more important than amassing ponderous conventional forces.

Determining how best to maintain security in this new environment is difficult for a policy establishment that has been deeply shaped by the past and that remains wedded, to a surprising degree, to old threats, old alliances, and old strategies. Cybersecurity is the best example of our difficulty in coping with new kinds of threats. In 1998, a presidential commission reported that protecting cyberspace would become crucial for national security. In effect, this advice was not so much ignored as misinterpreted—we expected damage from cyber attacks to be physical (opened floodgates, crashing airplanes) when it was actually informational. To meet this new threat, we have relied on an industrial-age government and an industrial-age defense. We have deferred to market forces in the hope they would produce enough security to mitigate national security threats. It is not surprising that this combination of industrial organization and overreliance on the market has not produced success. As a result, there has been immense damage to the national interest.

The damage from cyber attack is real. In 2007, the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities. The unclassified e-mail of the secretary of defense was hacked, and DOD officials told us that the department's computers are probed hundreds of thousands of times each day. A senior official at the Department of State told us the department had lost "terabytes" of information. Homeland Security suffered break-ins in several

of its divisions, including the Transportation Security Agency. The Department of Commerce was forced to take the Bureau of Industry and Security off-line for several months, and NASA has had to impose e-mail restrictions before shuttle launches and allegedly has seen designs for new launchers compromised. Recently, the White House itself had to deal with unidentifiable intrusions in its networks. Senior representatives from the intelligence community told us that they had conclusive evidence, covertly obtained from foreign sources, that U.S. companies have lost billions in intellectual property.[5]

The evidence is both compelling and overwhelming. Ineffective cybersecurity and attacks on our informational infrastructure in an increasingly competitive international environment undercut U.S. strength and put the nation at risk.

Our most dangerous opponents are the militaries and intelligence services of other nations. They are sophisticated, well resourced, and persistent. Their intentions are clear, and their successes are notable. Porous information systems have allowed our cyberspace opponents to remotely access and download critical military technologies and valuable intellectual property—designs, blueprints, and business processes—that cost billions of dollars to create. The immediate benefits gained by our opponents are less damaging, however, than is the long-term loss of U.S. economic competitiveness. We are not arming our competitors in cyberspace; we are providing them with the ideas and designs to arm themselves and achieve parity. America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage.

Exploiting vulnerabilities in cyber infrastructure will be part of any future conflict. If opponents can access a system to steal information, they can also leave something behind that they can trigger in the event of conflict or crisis. Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks. Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict.

The problem is not simply data confidentiality and service availability; the integrity of information stored on digital networks is also a target. The use of cyberspace has become a central element for many companies' business plans—how they manage their supply chains and their internal services and how they work with their customers. Scrambling data and information can also provide real military benefit: the United States uses blue-force tracking that tells commanders

[5] See "Threats Posed by the Internet," from the first phase of our work; it is on the CSIS Web site at http://www.csis.org/media/csis/pubs/081028_threats_working_group.pdf.

where friendly forces are located; imagine if an opponent could randomly turn some of the blue signals to red or make some of the red-force tracking disappear. The central problem for our opponents is not how to achieve this kind of disruption but to decide which disruptive option to pursue among the wealth of attack opportunities we offer them.

This situation and the losses it entails are not tolerable. A serious national security strategy cannot ignore it. The Commission on Cybersecurity for the 44th Presidency, a group of experts with a wide range of knowledge, has identified actionable recommendations for the next administration to repair this. Our goal has been to find both immediate and long-term steps that a new administration can take to increase costs and risks for cyber attackers and reduce the benefits they gain. The United States must ensure that it benefits from advances in information technology, manages its own risks, and increases the costs and risks faced by any cyber attackers.

The need to develop a coherent and strategic response to the cyber threat also presents the United States with a tangible opportunity. Our government is still organized for the industrial age, for assembly lines and mass production. It is a giant, hierarchical conglomerate where the cost of obtaining information and making decisions is high when this requires moving across organizational boundaries. There is a more efficient way to govern. We found new models in the experience of the private sector, where networks and technology have allowed companies to test news ways for their employees and partners to work together. The use of information technology and networks by large organizations to increase information sharing and collaboration raises productivity, lowers costs, and improves performance.

What we have discovered in the course of our work is that the organization of the federal government, which dates to the 1930s or earlier, is part of the reason we are vulnerable. A strategic approach to security requires reorganization. Our principal recommendations for security do not call for a supercop but for a strategist who, under the direction of the president, can plan and implement the move to a secure, information-age national government. Creating the organization and policies needed to begin this change will not be easy, but the nation that seizes this opportunity first will gain immense competitive advantage over others.

When our Commission began this effort in August of 2007, the United States had suffered a wave of cyber penetrations that afflicted many U.S. agencies, including State, Defense, Commerce, and NASA. In response, the Bush administration announced a new and important cyber initiative. Although much of the initiative was highly classified, we have amended our work when necessary to take the initiative into account.

Let us be clear on the Bush administration's Comprehensive National Cybersecurity Initiative (CNCI): It is good but not sufficient. The next administration should not start over; it should adopt the initial efforts of the initiative, but it should not consider it adequate. The CNCI has its focus on defending government—.gov, in other words—an approach that skilled opponents will be able to outflank. In key areas for cybersecurity—strategy, broad military doctrine, critical infrastructures, regulation, identity—there is no corresponding effort in the CNCI. Despite the CNCI, we were encouraged by efforts of senior officials at the Departments of Defense and Homeland Security and at the Office of the Director of National Intelligence to develop recommendations for a coordinated, strategic approach by the U.S. government to the problem. This is the central focus of our work.

We began with one central finding: The United States must treat cybersecurity as one of most important national security challenges it faces. Cybersecurity can no longer be relegated to information technology offices and chief information officers. Nor is it primarily a problem for homeland security and counterterrorism. And it is completely inadequate to defer national security to the private sector and the market. This is a strategic issue on par with weapons of mass destruction and global jihad, where the federal government bears primary responsibility.

Note that throughout our work we were cognizant that the rationale for securing cyberspace involves not only national security; it also involves safeguarding our democratic traditions and the protections afforded by our Constitution. This is our second major finding: that greater security must reinforce citizens' rights, not come at their expense. In meeting the challenge of securing cyberspace, our nation can reaffirm and reinforce its values, and we oriented our recommendations to achieve this.

1
Create a Comprehensive National Security Strategy for Cyberspace

Recommendations

- The president should state as a fundamental principle that cyberspace is a vital asset for the nation and that the United States will protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public.

- The president should direct the National Security Council (NSC), working with a new office in the Executive Office of the President (EOP)—the National Office for Cyberspace—and other relevant agencies to create a comprehensive national security strategy for cyberspace. Comprehensive means using in a coordinated fashion all the tools of U.S. power—international engagement and diplomacy, military planning and doctrine, economic policy tools, and the work of the intelligence and law enforcement communities.

- The United States should open the discussion of how best to secure cyberspace and present the issues of deterrence and national strategy to the broad national community of experts and stakeholders.

The next administration has an opportunity to recast U.S. strategy to fit a changed international environment. Pragmatic engagement and the use of all attributes of U.S. power can increase the safety and prosperity of our own nation and other nations. However, the task of recasting strategy comes at a difficult time. Our influence as a nation is at its lowest point in decades. Our international relations are in disarray. Years of underinvestment have weakened both government and our scientific establishment (and, in the case of government, scorn from those who sought to shrink it). The reputation of the United States has been badly tarnished, and our failure to defend cyberspace, despite huge informational losses, has encouraged our opponents to increase their attacks. The next administration can remedy the situation when it creates its own national security strategy and, in doing so, can use cyberspace to regain national strength and advantage.

Strategies articulate goals and identify the means to achieve them. The United States has clear goals—to defend itself and its allies from threats and intimidation, increase openness to trade and to ideas, and expand the rule of law

and of democracy. The most important goals for national security are, of course, to defend the national territory, protect the American people, and create an international environment conducive to peace and opportunity.

To advance these goals we recommend a clear articulation of the importance of cyberspace to the nation. The president, as one of his earliest actions, should make a statement of fundamental government policy for cyberspace. This statement should make clear that cyberspace is a vital national asset that the United States will protect using all instruments of national power.

To some extent expressing principles for cyberspace is more difficult than expressing a military doctrine designed to protect our physical territory. The Internet is part town square (where people engage in politics and speech), part Main Street (where people shop), part dark alleys (where crime occurs), part secret corridors (where spies engage in economic and military espionage), and part battlefield. As a result, we recognize that any fundamental principle or "doctrine" related to the Internet will affect all aspects of U.S. life and must be carefully crafted. This fundamental principle will provide the basis for a new national security strategy on cyberspace.

The benchmark for national strategy is the grand strategy adopted for the Cold War. That strategy grew out of a deliberative process in the Eisenhower administration that included a careful weighing of different options. The central elements of this strategy remained in use for the next 30 years. This reflected both careful planning and the stability of the international environment, where the principal threat to U.S. security remained essentially the same for decades.

Perhaps it is unrealistic to expect a similarly broad and enduring strategy for a very different environment, where the pace of change is much more rapid. There has also been reluctance, since the end of the Cold War, to undertake a serious review of strategy because this could involve questioning some very comfortable assumptions about the place of the United States in the world and how other nations view us. We are not indispensible, a hegemon, or unchallenged, and the evolution of cyberspace clearly reflects this.

That said, the United States faces serious threats and challenges that a national strategy must deal with: violent extremism in support of a radically different worldview; the emergence of powerful new state competitors; the global interdependence of economies and networks; and the spread of technologies that provide military advantage, which in an earlier time were available only to nation-states.

Among the technologies that are widely accessible are those that allow for operations in cyberspace. Cyber attack joins terrorism and weapons of mass destruction (WMD) as one of the new, asymmetric threats that put the United States and its allies at risk. A comprehensive national security strategy must

address cybersecurity. A comprehensive cybersecurity strategy must engage all elements of U.S. power—economic, diplomatic, and law enforcement as well as military and intelligence.

As with the larger national security strategy, we identify four principal instruments—international engagement, military and defense actions, economic tools, and the coherent use of intelligence and law enforcement capabilities—to achieve this. Marshaling these four sets of activities for a common purpose is difficult, and the need for a coherent, coordinated approach helps explain our preference for placing ultimate responsibility for cybersecurity in the White House's NSC, which has more authority and experience than any agency in promoting the coordinated implementation of presidential strategies.

One model for the new approach, which we recommend for the next president, can be found in the U.S. experience with nonproliferation and WMD. Twenty years ago, the proliferation of WMD was often an afterthought in discussions of the strategic environment. With the end of the Cold War and the reprioritization of U.S. strategy, the profile of nonproliferation in national security grew rapidly. After 1989, the president created an NSC directorate and issued new policies and directives, and Congress passed legislation providing authorities and sanctions; regulations were published and the Department of State (DOS), the Department of Defense (DOD), and the intelligence community established offices to deal with the new challenge. Internationally, the United States created new multilateral organizations for coordinated action against WMD, reenergized existing ones, and made nonproliferation a norm for international behavior and a factor in every major initiative. Nonproliferation went from being a relatively minor part of U.S. national strategy to become one of its most critical elements. Although the risks and requirements are different for cyberspace, the trajectory of WMD during the past two decades offers a useful precedent for how the next administration can approach this new challenge.

Every president since Franklin Roosevelt has defined and made public a national security strategy that identified key U.S. interests and laid out the means to achieve them. With our increased reliance on information technology, it is now time for cyberspace to be a central part of the next president's national security strategy. Its treatment must be consistent with the broad strategic goals we as a nation have pursued for decades—to defend the nation, advance U.S. interests, and protect allies. The next president must secure cyberspace for the free exchange of ideas and commerce and to protect critical national assets (both infrastructure and information) from damage or attack. Our recommendations call for the use of all instruments of U.S. power to undertake this task.

International Engagement and Diplomacy

Cyberspace spans the globe. No single nation can secure it, and any strategy centered on domestic action will be inadequate to address a global challenge. The international aspects of cybersecurity have been among the least developed elements of U.S. cybersecurity policy. Given the multinational and global aspects of network security, this must be remedied, as energetic engagement could produce real benefits in promoting U.S. objectives and reducing risk. Achieving this energetic engagement requires a coordinated international plan that would make use of all the international tools available to the United States. Much of this task will fall on the DOS, and the White House will need to ensure that other agencies incorporate cybersecurity advocacy into their international activities.

Our vision of an international strategy involves advocacy, cooperation, norms, and deterrence. The first step is for the president to issue a policy directive—based on the country's larger and public cybersecurity strategy—that lays out objectives, assigns agencies their cyber missions, and weaves cybersecurity into the nation's international efforts. The goal is to make the most of opportunities to incorporate cybersecurity commitments into many kinds of bilateral and multilateral projects just as the United States has broadly advocated measures to advance nonproliferation or to combat terrorism. Much of this task will fall on the DOS, and the NSC will need to ensure that other agencies incorporate cybersecurity into their international activities as well.

We recommend that the United States advocate measures to secure cyberspace in every multilateral initiative where it is appropriate, just as we have advocated measures to advance nonproliferation or to combat terrorism. There are many opportunities for bilateral or multilateral advocacy. Better cybersecurity should be part of the Department of the Treasury's work on financial payments systems in developing economies. When the Department of Health and Human Services or the Centers for Disease Control and Prevention build health information systems with foreign partners, cybersecurity should be emphasized. There is an opportunity when the Federal Reserve Board works with the Bank for International Settlements and the Electronic Banking Group to secure electronic banking systems. When the U.S. representative at the World Bank reviews a plan for cooperation with a developing nation, the representative should ensure that it contains commitments to improve that nation's cybersecurity.

The U.S. willingness to cooperate with other governments on cybersecurity matters will be an important component of U.S. advocacy. That cooperation should focus on establishing norms, which are expectations or models for behavior. There is an international norm, for example, against supplying WMD technology to others. Although norms are not legally binding, they can be codified in a regime (like the Missile Technology Control Regime) or a treaty (as

in the Council of Europe Convention on Cybercrime). A normative approach to international cybersecurity focuses on how countries should behave. Behavior by a country that is contrary to a norm often results in embarrassment or stigmatization. Today, norms for cybersecurity are weakly articulated, and enlisting a group of like-minded nations to develop and propagate such norms would improve security.

Norms can be reinforced by sanctions. The international component of U.S. cybersecurity strategy should include the development of sanctions for those countries that harbor cyber criminals or engage in cyber attacks. This would require the president to work with Congress to define appropriate sanctions and obtain the necessary authorities. Sanctions could be very broad, as with current sanctions on state supporters of terrorism, or narrowly targeted on specific entities, as is the case in the Iran Nonproliferation Act of 2000. Although the diminished stature of the United States will weaken any unilateral action, sanctions signal seriousness of intent to the international community and create thresholds for appropriate behavior and appropriate responses.

Some object that it is not in the U.S. interest to promote norms as this could hamper our own ability to operate, while other nations that have repeatedly demonstrated a willingness to ignore norms would not be constrained. Again, the WMD precedent is useful. Agreeing to certain restrictions on WMD did not greatly hamper U.S. operational capabilities, in part because the United States had developed the necessary military doctrines that could accommodate international norms. We will gain more than we lose in creating norms for cybersecurity.

The United States can strengthen its efforts to improve cybersecurity if it builds multilateral cooperation. As a first step, the United States should expand its work with allies (NATO, and more closely with the United Kingdom, Australia, and other close partners) on collective defense. Collective defense, in contrast with law enforcement cooperation, requires a deeper kind of cooperation and commitment among participating nations that goes beyond cyberspace. Collective defense in cyberspace provides some increase to deterrent capabilities—for example, knowing that an intrusion or attack on one nation will trigger responses from its allies or partners may lead attackers to reconsider and can increase the resources available for response.

A national security strategy for cyberspace will need to include both formal and informal efforts to engage internationally to improve global cybersecurity. For example, no nation can be an effective partner in fighting international cyber crime unless it has in place both the domestic laws and the operational expertise to do so—all of which it is also willing and able to put to the service of victims (or potential victims) in another country. Creating these partners worldwide means the United States should encourage nations to pass adequate laws and build

operational and technical expertise. Several important multilateral efforts already aim at this goal, but the next administration should make them a much higher priority.

The United States is already a party to the most important of these efforts, the Council of Europe Convention on Cybercrime. This multilateral treaty requires signatory nations to create the basic legal infrastructure that fighting cyber crime requires and to commit to assisting other signatory nations in investigating and prosecuting cyber criminals. At the same time, it respects our constitutional protections and privacy values. It is important to note, however, that while the convention establishes a legal baseline for effective cyber-law enforcement, many important countries have not yet ratified or signed it. Encouraging other countries to qualify for membership should be a diplomatic priority, which the United States should pursue bilaterally and through regional organizations such as the Asia-Pacific Economic Cooperation (APEC), the Organization of American States (OAS), and the Organization for Economic Cooperation and Development (OECD).

The OECD, the Group of Eight (G-8), APEC, the Council of Europe, and even the United Nations have cybersecurity initiatives, but there is no specific regime expressly focused on cybersecurity. A cyber regime, modeled on the Missile Technology Control Regime or the G-8's Financial Action Task Force (FATF), would bring together like-minded nations to develop international norms, common policies, and responses and to share sensitive national information on cybersecurity. This regime might initially include only NATO nations, Japan, Australia, and a few others. FATF comprises countries that have agreed to observe certain best practices for international financial transactions. FATF's goal is to make money laundering more difficult and more easily detected. The group develops best practices and standards and will not accept a new member until it has made progress in adopting them. Members who fail to live up to their obligations face sanctions from the financial community.[6]

Because FATF members have voluntarily agreed to follow best practices, many of the dilemmas found in proposals to devise a UN treaty to secure cyberspace are avoided. The problem with such a treaty is that many signatories are unlikely to live up to their commitments and the UN is politically incapable of enforcing a treaty. It is ironic that some of the countries that most vigorously advocate a UN treaty are known sanctuaries for cyber crime and are themselves suspected of launching cyber attacks.

---

[6] Financial Action Task Force, OECD, http://www.fatf-gafi.org/pages /0,2987,en_32250379_32235720_1_1_1_1_1,00.html.

Despite this, part of the next administration's task will be to find ways to work not only with like-minded nations, but with those nations that are indifferent and even our opponents, on those matters where there is some commonality of interest. This could involve creating a discussion forum with broad membership, open to all nations, to find areas where we can cooperate in security cyberspace. This would include potential opponents such as Russia, China, and others. Although any agreement on cybersecurity with nations such as these will be limited, it is essential to engage with all nations whose cyber activities make them important to the effectiveness of the broader U.S. cyber strategy.

Military Doctrine and Deterrence

Much of the discussion regarding the military aspects of cybersecurity is necessarily classified, thus limiting what our Commission can say on subjects such as offensive information warfare capabilities. However, just as a discussion of nuclear weapons can consider doctrine for their use or how best to employ them for deterrent effect without revealing classified details, certain essential topics relating to cyberspace are neither classified nor fully developed and can be discussed here. The most important of these is the need for a credible military presence in cyberspace to provide a deterrent against potential attackers. Although offensive cyber capabilities are not the only deterrent, possessing an offensive capability has a deterrent effect and the absence of an offensive capability makes deterrence a hollow threat. Sustaining an offensive capability will require providing adequate resources for training and equipping forces in cyberspace and developing the necessary military doctrine for their use.

We start with the recognition that DOD has made extensive progress in preparing for conflict in cyberspace. It is the best-prepared agency (along with components of the U.S. intelligence community) when it comes to cyber defense, and there has been significant movement in developing an offensive cyber capability, including the development of a classified military doctrine for cyber warfare.[7]

That said, and with adversaries increasing their cyber-warfare capabilities, the need for a credible and robust military presence in cyberspace is unquestionable. Absent that presence, the United States will remain at

---

[7] National Security Presidential Directive-16, July 2002. In addition, DOD is undertaking a complex reorganization of its cyber functions. This goes well beyond U.S. Air Force efforts to reorganize its cyber warfare structure, which traditionally maintained a degree of separation between computer network attack functions and the computer network defense and network management functions. The Air Force is considering unifying all aspects of cyber operations under United States Strategic Command (one of the 10 unified combatant commands), with offensive, defensive, and management components managed by a single integrated subcommand for cyber located at Fort Meade.

considerable risk. A military cyber capability is not the only possible deterrent to attack, but the absence of an ability to both defend and attack risks making other deterrence strategies a hollow threat. Having a credible military presence in cyberspace will require developing the necessary military doctrine for the use of forces.

Refining and expanding existing military doctrine is an essential step. Doctrine must be linked to the larger national strategy, and the United States must find ways to communicate both national policy and military doctrine to potential opponents. Doctrine is a military term. It is the principles by which a nation operates its military forces. It lays out other operational concepts for the employment of force. Outside of the military, the equivalent of doctrine for the government is found in presidential policy directives (variously known as presidential decision directives, national security policy directives, and homeland security policy directives [HSPDs]) and their associated documents. These documents define permissible actions and responses in cyberspace and provide the basis for development of more detailed supporting strategies to implement the president's policy.

Military doctrine for cyberspace is dependent on the larger cyber strategy. A comprehensive national strategy will allow the United States to go beyond military operations, specify relationships among agencies, and lay out the decisionmaking processes. As we have described in our recommendation for national strategy, it must cover international engagement, economic activities, intelligence, law enforcement, and defensive and offensive operations.

Military doctrine is crucial for guiding defensive and offensive actions and for expanding deterrence. For example: What kind of response is justified for an attack on critical infrastructure that we determine to have originated from a foreign government? How does our response differ if an attack involves a loss of information rather than disruption of a service? Military doctrine will need to provide guidance on the exercise of the various and overlapping legal authorities that apply to cyberspace, identifying when the use of law enforcement, military, or intelligence authorities is appropriate. The goal should be an evolving document that provides a template for action in cyberspace.

Military doctrine can provide a common perspective for training, planning, and execution of operations in cyberspace. It clarifies missions and responsibilities among agencies when they operate in cyberspace. This remains a weakness in U.S. efforts in cyberspace: while the national leadership believes that missions and command structures are clear, many of our interviews found continuing uncertainty among the operators. This may reflect, in part, overclassification, but the publication of a national security strategy would remedy this.

In addition, some larger doctrinal questions remain unanswered—specifically around preemption, symmetry, deterrence, and communications with opponents (signaling, in other words). To begin, does the United States include preemptive action as part of its cyber military doctrine? In other strategic contexts, we have rejected preemptive action (knowing that the Soviet Union had a nuclear capability did not lead the United States to seek to preempt it). Preemptive action can be inherently destabilizing, as it will appear as an attack to the target rather than as a defensive move. In some instances, however, preemption may be justified, but these instances would need to be clearly defined and linked to a clear chain of authority for approving preemptive action.

Military doctrine also needs to establish thresholds for response. When does an incident (or potential incident) in cyberspace justify either a preemptive action or retaliation? When does retaliation move from an act against the attacker to a larger network, when does it move from the attackers' network to another network located in the same country (such as an attack by an intelligence service that leads to a response against that nation's electric grid), and when does it move from action in cyberspace to physical action? Establishing thresholds for escalation is closely linked to deterrence—thresholds allow an attacker to better calculate the potential cost of an action. Thresholds are of course not rigid. The larger political environment shapes them, and decisions on responses ultimately must lie with political authorities. However, thresholds can and should be publicly known in general terms in order to maximize their deterrent effect.

Current efforts are ongoing to develop doctrine for deterrence, but they face significant impediments. Deterrence is hampered by uncertainty about the identity of the attacker, the effect of the attack, and the collateral damage that could accrue to innocent third parties. We also lack well-defined means to signal our intentions or doctrines for response to potential attackers in a way that would change their calculus of the advantages and risks of an attack. These uncertainties limit the value of deterrence for cybersecurity.

Deterrence in cyberspace is particularly complicated because of the problems with attribution and identification. If a country does not know who is attacking, it is difficult to create appropriate and proportionate responses in ways that reduce the chance of escalation. A signal that a country is contemplating a response that goes to all potential attackers will not deter and could actually create more conflict. Attacks come over a global network to which we are all connected, and the attackers can use unsuspecting civilian computer networks, assembled into botnets, to launch their attacks.

The 2007 attacks on Estonian networks are a good example of these problems. The attacks are widely attributed to Russia, yet there is no evidence to substantiate this. The attackers, a collection of cyber criminals and amateur

hackers mobilized and encouraged by unknown entities used captive computers around the world—in Europe, China, and in the United States. A counterstrike against the attacking computers would have damaged innocent networks in many countries and might not have affected the attackers at all. This is not much of a deterrent, and it is complicated by the incentive of attackers to disguise themselves and make it appear that an attack is coming from the third party—Russian hackers leaving tracks that lead up to Beijing, for example.

In light of the difficulties in attributing an attack, we may need to rethink how deterrence works in cyberspace. Instead of focusing only on counteractions, we may improve deterrence if we act and invest in order to ensure resiliency and continuity of service. If opponents believe that their attacks will have little effect, they will be less likely to launch them.

Deterrence is also hampered by the lack of a public strategy and military doctrine. The deterrent effect of an unknown doctrine is quite limited.[8] One of the main reasons we advocate the creation and articulation of a national cyberspace strategy, based on a fundamental principle articulated by the president, is for its deterrent effect. Strategy and military doctrine are also essential for signaling intent. The absence of explicit military doctrine complicates signaling. Signaling was a critical part of deterrence and strategic conflict during the Cold War, and it contributed to stability. It involves linkages between an action and a response: an internal U.S. linkage that a certain action will prompt a specified response; and an external linkage that the opponent understands that its initial action triggered the U.S. response.

A Soviet submarine, for example, might get too close to the U.S. coast (a closer position meant a shorter flight time for a missile, which meant that the shorter warning for the United States inherently reduced stability by increasing the chance of a surprise attack). In response, the United States might visibly move strategic bombers to a higher state of readiness at airfields in the middle of the country, fueling them and parking them on the flight line, ready to take off on very short notice. A Soviet reconnaissance satellite would detect this change in status, and the next day the submarine would draw away from the coast. In such a case, an exchange of information between potential opponents about discomfort and intent had taken place without any words or messages and without any potentially escalatory and politically difficult official communications.

---

[8] The current U.S. deterrent posture is reminiscent of the scene in the film, *Dr. Strangelove:* after the Soviet ambassador explains that the Soviets invented a doomsday machine to deter the United States from attacking, Dr. Strangelove responds by saying "Yes, but the whole point of the doomsday machine is lost if you keep it a secret! Why didn't you tell the world?" See Dan Lindley, "What I Learned since I Stopped Worrying and Studied the Movie," September 30, 2008, http://www.nd.edu/~dlindley/handouts/strangelovenotes.html.

Today we have no equivalent of that exchange in cyberspace. How do we signal to an adversary that we have detected an action that we consider threatening and are prepared to respond? Because we do not yet have well-established responses, we cannot signal our intent to use them, nor do we have clear rules of engagement that are known, in broad terms, to an adversary so that it can correctly interpret our actions. Given the newness of cyber warfare, we should not be surprised that there is no lexicon for strategic conflict in cyberspace, nor clear rules of engagement, nor a menu of responses, nor the means to signal intentions to potential opponents. The normal practice now is the keyboard-versus-keyboard or geek-versus-geek approach. This lack keeps the United States in a reactive position, responding to attacks after they occur rather than preventing them. Better security requires moving to a more comprehensive set of responses.

Symmetry is a related problem. Deterrence assumes some level of symmetry in the risks that attacker and defender nations face. The United States and the Soviets mutually held hostage their cities or their strategic forces. This symmetry is not present in cyberspace. Some nations are far less dependent than the United States on the Internet and other networks. A few nations, such as China, have developed Internet architectures that provide a degree of insulation from cyber attack. Finally, nonstate attackers face none of the constraints that operate on a nation-state. There is usually an assumption of symmetry in the level of force used in a response, but the most effective response to a cyber attack may not be with some counter move in cyberspace. This does not mean that deterrence will not work, but it means that for cyberspace (as opposed to nuclear war), defense may be more important than offense.

Deterrence, signaling, and a strategic lexicon took years to work out in the nuclear era. The next administration needs to establish a comprehensive national cyber strategy that provides a proactive approach to securing cyberspace and that guides military doctrine and other national policies. The goal should be an evolving public document that lays out the framework for action. Our recommendations are to refine and make public existing military doctrine and to create processes with a broad membership (beyond DOD, the intelligence community, and the information technology (IT)community) that can work through the issues of deterrence and strategic exchange in cyberspace.

A final point on military doctrine and deterrence is that there must be public awareness. One dilemma with the Comprehensive National Cybersecurity Initiative (CNCI), which was established in January 2008, was that it was highly classified and thus could not be easily shared with the public, industry, or even close allies. Many officials at all levels and from all agencies complained to us about overclassification and the complications it introduced. Eventually, the White House made public certain elements of the CNCI, but much remains

classified. We received classified briefings during our interviews, and in our opinion, only a few CNCI elements deserved any classification. In the era of nuclear deterrence, specific capabilities and plans were highly classified, but general knowledge of policies and weapons was widely available. Such openness is even more important in cybersecurity, given the large role played by those outside of the federal government.[9]

A credible military posture will require adequate resources for training and equipping forces in cyberspace. Anecdotal evidence suggests that we lag behind some of our competitors in this area. The lack of a defined career path also hampers cyber-warfare efforts. One problem we heard several times in our interviews with senior military officials was that after a "cyber warrior" is trained and gains experience, that person's next assignment may well be network management on a military base. It is not surprising that some individuals leave the service for better opportunities when this occurs. Developing a career path and training programs to create a dedicated cadre is an essential next step, and chapter 7 lays out recommendations for building a skilled force.

Economic Policy

The United States has made only sporadic use of the economic tools available to it for cybersecurity. Our recommendation is that the United States not underestimate the potential of these economic tools, for much economic power rests on the strength of U.S. industry in the global IT market. The United States does not dominate or control this market, but its companies play a central role in it and remain very influential in shaping the standards and products that define cyberspace.

Traditionally, the economic tools for international engagement have included aid, trade, and investment although these traditional tools are less useful now. Multilateral trade negotiations are in disarray, and the United States has lost influence in that arena. Bilateral trade negotiations could provide an opportunity for progress. During the past few years, for example, the United States has been engaged in negotiations with Russia on the conditions Russia must meet to win World Trade Organization (WTO) membership. The United States, along with the European Union, asked that Russia improve its business climate by taking such steps as improving intellectual property protections or opening its financial and service markets. The United States did not insist, however, that Russia take steps to reduce cyber crime or that Russia accept the Council of Europe Convention on

[9] We are mindful that the offensive use of cyberspace can potentially complicate collaboration with the private sector and other nations. Some partners may view information sharing with suspicion if they think we may use it to enhance offensive capabilities. The United States will need to develop confidence-building measures to mitigate this problem.

Cybercrime. Although it is too late to ask for Russian commitments as a price of WTO membership, commitments to improve cybersecurity and to work against cyber crime should become a routine part of our international negotiations.

Standards are the most important of these tools. Standards are formal rules for how products are made or how they should work. Standards and standard-setting processes have become particularly important for shaping cyberspace. As the United States directly participates in and can influence international standards bodies to improve security, all networks will benefit. Existing mechanisms, like the Common Criteria Recognition Agreement (a multilateral agreement and International Organization for Standardization [ISO] standard), offer an opportunity to build greater collaboration. Trade negotiations, by promoting common standards and by breaking down barriers to collaboration, will also improve security. The adoption of security-increasing procurement practices by the United States government, done with an eye to the global nature of the IT marketplace, will drive not only U.S. companies but also companies in other countries to improve their processes and products in response.

U.S. policies and actions on international Internet governance can also increase cybersecurity. Active engagement in both governmental and nongovernmental forums for Internet governance will safeguard U.S. interests and provide an opportunity for building multilateral cooperation to secure cyberspace. One focus for this activity is the nexus among the UN, the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU). In each of these areas, the United States faces problems.

How to move forward on ICANN, for example, remains a potentially divisive issue between the United States and other nations. The United States has lost influence in the ITU. This poses some risk that other nations or groups of nations could establish alternative mechanisms for Internet governance on the basis of political and economic interests that shrink the openness of cyberspace. The growth of "walled gardens" in the Internet would limit the global interconnectivity, commerce, and social dialogue the Internet has enabled to the detriment of U.S. interests. The U.S. goal must be to promote a cyberspace that is open and that provides global links. It is important that the U.S. government and U.S. companies engage internationally.

Finally, an economic strategy for cyberspace must include working to increase trust in the IT supply chain. IT is produced by a global supply chain that includes potential opponents, and it is sufficiently porous (or obscure) to provide the opportunity to make malicious changes. We cannot go back to a national supply chain, but for a few critical functions the United States will need to ensure that it retains sufficient manufacturing capabilities to supply trusted components

and software. Other initiatives—such as better authentication and secure product configurations (as discussed below)—offer ways to manage supply-chain risk. The United States can use acquisitions reforms (also discussed below) to help create incentives for IT producers to improve product security, and it can use bilateral agreements with foreign governments and industries to reduce supply-chain risk.

Intelligence and Law Enforcement

The final pillars of a comprehensive national cybersecurity strategy are intelligence and law enforcement. The intelligence community has been a leader in the efforts to improve cybersecurity. Its primary role in securing cyberspace will be to support diplomatic, military, and domestic elements of the strategy. It plays an essential role in developing an understanding of adversaries' intentions and capabilities; it can then provide that information to other agencies, trusted international partners, and, in some instances and in an appropriate form, the private sector. The intelligence community, given its unique authorities, is best suited to develop and deploy an early warning system for cyberspace, to detect and identify hostile foreign actions. Part of this early warning should include efforts to improve attribution, for without concrete attribution, deterrence is more difficult to achieve and sanctions impossible to implement.

The intelligence community of course has other functions in cyberspace, including the clandestine collection of information and covert action against opponents. These are essential for improved cybersecurity, and a national strategy will need to consider how to integrate the classified elements into a larger defense. The primary dilemma for intelligence entities is deciding when it is appropriate to use covert actions undertaken by the intelligence community to prevent or respond to a cyber attack and when to use the offensive capabilities developed by the military for cyber warfare. Traditional thinking in terms of peacetime-versus-wartime actions must be refined when working in cyberspace, particularly given its global context and its pace. The White House, military commanders, and intelligence organizations will need to accelerate decisionmaking if cyber defense is to be most effective.

The president's intelligence authorities allow broad discretion, but a national strategy will need to define intelligence and military missions, for example, who best should perform different kinds of covert actions and how national authorities should authorize such actions. The president should ensure that both the military and the intelligence community expand their offensive capabilities under an appropriate framework for the authorization of covert action. A presidential directive could provide the framework for covert action in cyberspace that

clarifies when military commanders are authorized to respond and when, as required by law, covert action is authorized by a formal presidential finding.

Any successful effort to secure cyberspace will be marked by the ability of law enforcement to identify and prosecute cyber criminals. Federal law enforcement agents and prosecutors along with their counterparts in state and local governments have made great strides in their capacity to trace network crimes back to specific criminals and hold them accountable worldwide. But this is an extremely difficult problem, and much work needs to be done—both to improve available expertise and to coordinate among investigating agencies.

Some of the network attacks and penetrations investigated by law enforcement may turn out to stem from intelligence targets or even nation-state actors, which will call for intelligence or even war-fighting measures rather than criminal prosecutions.[10] But the United States must first diagnose and attribute the attack or penetration before making those decisions, and sometimes it may be necessary to employ several responses at once.

Partly because these cases are so difficult, some victims in the private sector and even on government networks have been reluctant to report attacks and penetrations to law enforcement, which diminishes the potential power of law enforcement. That said, nothing upends an attack quite so decisively as arresting the person who is committing it; nor could technical experts hope for a better diagnostic and network repair tool than data seized by law enforcement on the attacker's own computer. The criminal hacker community pays attention when other computer criminals are caught and punished.

Investigating who did what to whom over a network is difficult, not only because the evidence is highly technical but also because it is frequently scattered across a globally networked crime scene. National law enforcement agencies cannot succeed in piecing it together without investigative support from their foreign counterparts, who have been key to many prominent multinational success stories, including breaking rings that targeted U.S. financial systems. The goal is to shrink the sanctuaries available from which cyber criminals attack anywhere in the world with impunity. Improvements in the legal regime for government (and multinational) access to data in cyberspace will help improve collaboration with foreign partners.

The United States is already a party to the most important of these efforts, such as the Council of Europe Convention on Cybercrime and the G-8 Subgroup on High-Tech Crime. The G-8 has made helpful operational contributions in the fight against cyber crime. Through U.S. leadership of the subgroup, it has

---

[10] Law enforcement should not be involved in counterattacks, as its primary function is to investigate and prosecute cyber crimes whether committed by individual criminals, organized crime groups, or a government agent.

established a points-of-contact network that allows investigators in more than 45 countries to reach each other day or night to collaborate on investigating network crimes. This operational network has had many successes in tracing the sources of crimes facilitated on global networks, but it is essentially an informal effort. The United States should work to expand, support, and formalize it by international agreement.[11]

One essential function for the U.S. Department of Justice is to ensure adequate protections for privacy and civil liberties in any cyber initiative. Acceptance of a more robust program will depend in some measure on the ability of the government to assure the public that its rights are being safeguarded. This assurance requires a commitment from the White House and scrutiny by the Department of Justice and by other independent agents (including the inspectors general, Office of Management and Budget [OMB], and potentially a revitalized presidential Privacy and Civil Liberties Oversight Board) of proposed actions, in combination with vigorous congressional and judicial oversight.

Establishing a fundamental national goal for cyberspace and creating a comprehensive national strategy to achieve it will vastly improve our performance in cybersecurity. This strategy must be complemented, however, by organizational changes that reinforce a comprehensive approach. As we considered a comprehensive cyber strategy, we realized that strategy and organization are linked. Just as the National Security Act of 1947 created new entities and agency relationships to meet the security challenges of that era, we believe that it is time to reorganize for cyberspace.

[11] The Council of Europe Convention on Cybercrime in Article 35 establishes an around-the-clock point-of-contact network.

2
Organizing for Cybersecurity

Recommendations

- The president should appoint an assistant for cyberspace and establish a Cybersecurity Directorate in the NSC that absorbs existing Homeland Security Council (HSC) functions.

- A new National Office for Cyberspace (NOC) would support the work of the assistant for cyberspace and the new directorate in the NSC. The president can create this office by merging the existing National Cyber Security Center (NCSC) and the Joint Inter-Agency Cyber Task Force (JIACTF).[12] The assistant to the president for cyberspace would direct the NOC.

- The NOC, with the new NSC Cybersecurity Directorate and the relevant agencies, would

  – Assume expanded authorities, including revised Federal Information Security Management Act (FISMA) authorities, oversight of the Trusted Internet Connections (TIC) initiative, responsibility for the Federal Desktop Core Configuration (FDCC) and acquisitions reform, and the ability to require agencies to submit budget proposals relating to cyberspace to receive its approval prior to submission to OMB;

  – Manage both a new federated[13] regulatory approach for critical cyber infrastructures and a collaborative cybersecurity network across the federal government;

  – Help develop the national strategy and oversee its day-to-day implementation and the performance of agency elements in securing cyberspace.

- The president should create three new public-private advisory groups to support the assistant for cyberspace and the NOC.

---

[12] The JIACTF was created by the director of national intelligence (DNI) to execute DNI responsibilities in monitoring and coordinating the CNCI and to report quarterly to the president on CNCI implementation, together with such recommendations as deemed appropriate.

[13] A federated approach involves individual agencies having some of their actions coordinated by a central authority. Those agencies continue to manage their policies and regulations, but they do so according to a common set of standards developed in a process coordinated by the central authority—in this case, the NOC.

- Existing agencies should keep responsibility for their current operational activities, with the Department of Homeland Security (DHS) continuing to be responsible for the United States Computer Emergency Readiness Team (US-CERT), and the US-CERT Einstein program, under the oversight of the NSC and the new EOP cyberspace office. OMB would maintain oversight of the budget functions in coordination (as it does for other policy areas) with the NOC and the NSC.

Twenty years ago, all the federal experts who protected cyberspace, gathered together, would have made a rather small club. Today, hundreds of cyber experts of varying ranks are found all over government—a proliferation in numbers that reflects the growth of the Internet itself and our reliance on it. But, although cyberspace operates with a shared set of organizing principles, the human network too often resembles a large fleet of well-meaning bumper cars.

The central problems in the current federal organization for cybersecurity are lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. A new administration could put much time and effort into an attempt to revitalize or resuscitate the existing organizational structure, which was the product of a marriage between a decade-long process of accretion and an end-of-term response to crisis. Our view is that this effort would waste time and energy.

The Commission considered many options for how best to organize for cybersecurity. We grew to understand the importance of bridging across the federal agencies in order to leverage the knowledge to provide the best security for our nation. Improving cybersecurity will be difficult, as the problem cuts across agency responsibilities. We also recognized the importance of involving the private sector—the federal government cannot do this alone.

Many of our interviewees encouraged us to think of a holistic approach to cybersecurity, one that looked beyond security alone and asked how best to enable and assure essential services in cyberspace. The progression of our thinking led from an improved DHS to an expanded cybersecurity function in the NSC; from an expanded NSC to a new cybersecurity entity; and from a new cybersecurity entity to one that looked broadly at enabling the secure and reliable use of cyberspace for national functions.

Our thinking on organization tracks with our finding that cybersecurity is now a central problem for national security. Our recommendation is to create a new "enterprise" governance model for cyberspace using the NSC, a collaborative network among the key agencies, and a new cyberspace office in the EOP.[14]

[14] An "enterprise architecture" restructures a corporation to work as a single entity rather than a collection of different business units. An enterprise structure is flatter, with fewer layers between

We based our recommendations in part on the intelligence community's experience in implementing the Intelligence Reform and Terrorist Prevention Act (IRTPA). IRTPA imposed a new, more collaborative structure on the intelligence community. It mandated a distributed "intelligence enterprise." Congressional mandates, however, are not enough. It took a director of national intelligence (DNI) with the appropriate authorities to build collaboration. This did not mean that the DNI became a centralized manager of the intelligence community—agencies still have their unique operational functions. The DNI role is as a strategist and builder, providing the strategy and collaborative networks for the intelligence enterprise. This effort, although it is still a work in progress, helped to guide our thinking.

What about the Department of Homeland Security?

One of the first tasks for the new administration will be to strengthen DHS. We had a long and impassioned debate within the Commission over DHS's roles and responsibilities. Many felt that leaving any cyber function at DHS would doom that function to failure. DHS is stronger in 2008, but even if DHS were strengthened further (and some in the Commission believe this could be done rapidly), the nature of our opponents, the attacks we face in cyberspace, and the growing risk to national and economic security mean that comprehensive cybersecurity falls outside the scope of DHS's competencies. DHS is not the agency to lead in a conflict with foreign intelligence agencies or militaries or even well-organized international cyber criminals.

Securing cyberspace is no longer an issue defined by homeland security or critical infrastructure protection. This is far too narrow a scope. Cybersecurity is no longer (if it ever was) a domestic issue. It is an issue of international security in which the primary actors are the intelligence and military forces of other nations. Cybersecurity requires harnessing U.S. international efforts, along with offensive capabilities and strong intelligence action to support a comprehensive national security strategy. Managing a complex international effort involving several large and powerful departments would be difficult for any agency, much less one that is still in the process of organizing itself. Although the department's performance has improved in recent years, our view is that any improvement to the nation's cybersecurity must go outside of DHS to be effective. For that reason, we recommend that the White House, rather than any single agency, lead the new strategic and coordination functions required for cybersecurity.

---

the chief executive officer and employees. Computer networks and software can enable the enterprise architecture by connecting many independent pieces into a single corporate network.

A New Executive Branch Structure

Simply appointing a cyber czar will not work. Czars in Washington tend to be temporary or marginalized. Longing for a czar is a symptom of our industrial-age governmental organization, where rigid organization lines are apt to produce interagency competition and paralysis. The implementation of the IRTPA, which imposed a new, more collaborative structure on the intelligence community, shows that the combination of a congressional mandate, adequate authorities, and a focus on "enterprise" solutions (that is, those that cut across traditional agency barriers) can improve federal performance.

We considered many alternatives for the best management of a comprehensive cybersecurity effort. The intelligence community has the necessary capabilities, but giving it a lead role poses serious constitutional problems, given the domestic interactions a comprehensive approach would require. DOD is well suited to manage a national mission, but giving it the lead could suggest a militarization of cyberspace. We also looked at Federal Bureau of Investigation (FBI), General Services Administration, or the creation of a small, stand-alone agency, and we decided that each of these alternatives had drawbacks. We concluded that only the White House has the necessary authority and oversight for cybersecurity. Our recommendation is to reorganize the federal effort at securing cyberspace. Our new structure has four elements:

- An assistant to the president for cyberspace, who directs and is supported by a new office in the EOP—the National Office of Cyberspace. This office would be small (10 to 20 people) and would provide programmatic oversight for the many programs that involve multiple agencies. It would absorb the coordination and oversight responsibilities of the National Cyber Security Center (NCSC) currently appended to DHS and give it additional functions and authorities.

- A merger of the NSC and the HSC to create a new directorate that (in addition to the NSC's current offensive cyber responsibilities) provides coordination with other agencies around national cyberspace policy and strategies.

- Three new private-sector advisory bodies to replace existing groups.

Because cybersecurity requires coordination of activities across agencies, the White House is the best place to locate this function. It alone has the authority to ensure coordination. The most appropriate place in the White House is the NSC. Cyberspace is now a major national security issue. The United States should treat it as such, following the precedent of WMD and nonproliferation. We recommend

that the president create a new assistant to the president for cyberspace, who will direct a staff within the EOP. The incumbent will also serve as a deputy national security adviser, participating in NSC meetings when appropriate and supported by a new NSC Cybersecurity Directorate. As part of the discussions with Congress on cyberspace authorities, the appointee to the position of assistant to the president could be set up to be confirmed by the Senate.

The NSC is the organization best able to coordinate a national security strategy and the international, military, diplomatic, intelligence, and law enforcement activities it entails. We do not recommend locating the new position in the HSC. In fact, we recommend that the next administration merge the HSC into the NSC. The split between "homeland" and "foreign" makes no sense for cybersecurity and in a globalized world makes little sense for U.S. security in general.[15]

Congress created the HSC, and legislative change is required to abolish it. While working with Congress to change this, the president can "dual hat" the White House staff to produce a de facto merging of the two organizations. Some worry that this could produce a militarization of cybersecurity. This reflects a fundamental misunderstanding of the nature of the NSC and its many regional offices—its job is to coordinate international relations and national security activities to ensure the president's policies are followed. We again point to the precedent set by WMD and nonproliferation—a strong NSC directorate forms the core of successful implementation of strategy.

National Office for Cyberspace

A strong NSC directorate is an important element of any improved governance structure, but by itself it is not sufficient. As we considered all the elements that an adequate cyber program would entail, we realized that a directorate of 15 or more people devoted to this single issue would swamp the NSC (or OMB). In addition, some on the Commission were uncomfortable with assigning an operational role to the NSC.

Only the NSC can ensure the integration of cyberspace into the larger national security strategy. The NSC, however, cannot assume the programmatic and management functions required for comprehensive cybersecurity, if only because an adequately sized cybersecurity office would dwarf the other directorate staffs in the NSC. Most administrations have chosen not to make the

[15] The concept of homeland security emerged in the 1990s, as the United States grappled with what the security environment would look like after the Cold War. The basic idea—that U.S. national territory would now face greater threat from asymmetric attacks such as terrorism, WMD, or cyber threats—was sound, but there were implicit weaknesses in segregating homeland from international security and in underestimating the scope and pace of global economic interconnection.

NSC operational[16]—a kind of super agency, in other words. Yet we concluded that management of a comprehensive program for securing cyberspace would fail if it were not in the White House—too many powerful agencies are involved and too many programs require deep and continuous coordination for any single department to effectively manage this problem.

In similar situations, the president has worked with Congress to create a new office in the EOP. Thus, we recommend that the president establish a National Office for Cyberspace in the EOP. This office would be responsible for some of the functions currently performed in other agencies, including DHS; and, once operational, the NOC would relieve some of the pressure on the NSC and OMB. As an interim measure, the president could create an Office of Cyberspace via executive order, while working with the Congress to authorize and fund a permanent entity. The assistant to the president for cyberspace would direct the NOC. Its functions would be to:

- Provide strategic direction and coordination on cyber defense and offense;
- Monitor and assess federal agency priorities, programs, policies, and budgets for cybersecurity;
- Develop new measures as necessary to improve the security and reliability of critical information infrastructure, including regulation and multilateral agreements;
- Provide a focal point for the private sector to coordinate on cybersecurity; and
- Ensure all programs are consistent with U.S. law and respect privacy and civil liberties.

There are many precedents for such an office, including the Office of the United States Trade Representative, the Office of Science and Technology Policy, and even, after 9/11, the Office of Homeland Security. The Y2K experience provides a particularly salient precedent, during which the White House appointed an assistant to the president who chaired the President's Council on the Year 2000 Conversion and whose work in coordinating and directing the U.S. response was supported by a small EOP office.

We were attracted to a division of labor between the NSC and a new managerial office in the EOP. The NSC would develop strategy and ensure

[16] By operational, we mean actions that respond directly to specific, ongoing problems and attacks.

coordination among DOD, DOS, the intelligence community, and other relevant agencies; this is the traditional NSC role. But the NSC should not be operational. Instead, the new office would manage the implementation of the strategy and provide oversight and direction, particularly for the many cyberspace-related programs that cut across traditional agency responsibilities. Both the directorate and the NOC would report to the assistant to the president for cyberspace.

Fundamental sources of power in the bureaucracy include access to the president, legislative authorities, and control of budgets. Any new entity responsible for securing cyberspace needs all three if it is to succeed. We designed our proposed new office with these fundamentals in mind.

The core of the NOC would come from the interagency staff currently providing coordination and monitoring functions for the CNCI. During 2008, this 20-person staff has provided programmatic oversight and reported to the White House on CNCI programs. Moving this staff into the new EOP office would provide immediate capability for the new administration as it establishes its own priorities and strategies. This move would also allow the NOC to assume responsibilities currently exercised by HSC, NSC, and the OMB for implementing the CNCI.

The NOC should also absorb the National Cyber Security Center (NCSC)—its staff, funding, and mission. The NCSC currently reports to the secretary of Homeland Security (through other DHS offices), is housed in DHS, and is staffed by a few detailees. Its mission is to improve coordination and communication among the six major government cybersecurity centers. Some officials we interviewed said they modeled it on the National Counter Terrorism Center (NCTC). If so, NCSC is only a pale reflection of the NCTC. NCTC was established by law and has statutory authorities. NCSC has no similar authorities. The NCTC director can raise issues directly to the president when necessary. We propose putting the NCSC on solid footing by moving its planning, integration, and oversight roles to the EOP and giving these key functions the staff and authority needed for these missions.

The NOC would be responsible for overseeing the implementation of national cyber strategies in support of the administration's cyber policies, including securing critical cyber infrastructures. The NOC would lead policy and coordination for legislative requirements, in particular FISMA and the Clinger-Cohen Act. These authorities would give the NOC responsibility for "standards, guidelines, and associated methods and techniques for computer systems." OMB currently leads these functions, but a lead role for an expanded cybersecurity mission would distort the nature of OMB and change its focus from federal budget and management to national security issues. We recommend the president

transfer this function to the NOC in order to give it "teeth" in the interagency process.

The NOC would work with OMB to evaluate cyber-related funding and programs across the federal departments and agencies. Specifically, the NOC would recommend new and redirected cyber program elements and activities used across domestic budget programs, the National Intelligence Program, the Military Intelligence Program, Information Systems Security Program, and other cyber-related programs. It would work closely with OMB and with the appropriate congressional committees to develop a coherent funding approach for cyberspace.

The NOC would be responsible for leading the development and overseeing the implementation of a national cyberspace strategy, including securing critical cyber infrastructures. The authorities of the new office should clearly provide oversight for other domestic agencies working with critical cyber infrastructures. The office would also provide the oversight and reporting that summarized the effectiveness of current programs, funding commitments and executions, and performance measurements; and it would make recommendations to reprioritize programs to ensure an efficient and effective federal cyber program for the security of the United States.

While the NOC would provide policy guidance and oversee implementation, we recommend that most operational functions remain with the agencies currently responsible. For example, the responsibility to collect and analyze real-time data from the Einstein effort, which could require dozens of analysts and support personnel, should remain the responsibility of DHS, as should US-CERT (although US-CERT would benefit from increased resources). The NOC should not seek to capture and own all federal efforts but should support them and ensure they progress to meet national needs. The experience of DHS points to the long-term disruption created by agglomerating functions in a new agency.

One of the most important functions of the NOC would be to create and manage a collaborative network for cybersecurity. This network must reach across government agencies and connect those with expertise and responsibility for cybersecurity. The existing interagency process is insufficient. It is too slow, too formal, and too centralized, and it has a tradition of pitched battles among agencies. The NOC would map expertise across the government and establish the collaborative tools (wikis and social networks, for instance) that will enable a new horizontal approach to addressing cyber problems. The precedent for this is the work of the intelligence community as it has used Intellipedia, Analytic-Space (A-Space), and other social networking tools to build an enterprise approach. The goal for the NOC should be to create a similar federal enterprise for cybersecurity.

Some call these tools Web 2.0. Behind the jargon, there is value. Executives at a number of companies (and at DOD) told us that using Web 2.0 social

networking tools increased risk, but the corresponding increase in productivity justified the exchange. Executives told us that their companies have incorporated blogs, wikis, and access to social networking sites deeply into their business operations, using a new business model that profitably let customers and partners participate on company networks. These executives also told us that if companies tried to restrict access, their most innovative and productive employees would leave for companies without similar restrictions.

Our proposed management structure would enable a collaborative social network among the offices and functions involved in cyberspace. Almost every part of the executive branch will have some role in responding to this threat, be it administering networks, responding to incidents, or setting priorities for the national research agenda. Each community's core expertise intersects with others. The NOC must draw on private-sector experience to find new ways to ensure that government efforts are coordinated far more effectively than is done today.

Toward an Information-Age Government

Building a collaborative network could be a first step toward a new kind of government. Our industrial-age organization makes a cyber-dependent government vulnerable and inefficient. A collection of hierarchical "stovepipes" is easier to attack and harder to defend because security programs are not of equal strength (the weakest link compromises all) and stovepiped defenders cannot appreciate the scope of, and respond well to, a multiagency attack. Cybersecurity strategy will need to look beyond a purely defensive posture and find new ways to increase security while improving the effectiveness, efficiency, and transparency of government operations. We believe that the next administration's response to the cybersecurity challenge provides an opportunity to test new approaches to federal organization that use cyberspace and social networking technologies to improve government performance.

Our recommendation to create the NOC came from discussion of whether it is time for the federal enterprise to have a chief information officer (CIO). In most large corporations, the CIO reports to the chief executive officer in recognition of the importance of information in the modern corporation. In the federal government, the so-called CIO is located in OMB, several layers from the president. Incumbents in this position have performed well, but we wondered whether it was time to move to models derived from successful experiments in the corporate world. There was strong belief that the CIO role is inextricably tied to overseeing security in cyberspace, and we were attracted to the idea of creating an office that begins to build integration across the federal agencies, that removes impediments to collaboration, and that emphasizes the importance of intangible factors for improving federal performance information. The NOC can provide a

test bed for the next president to experiment with how best to organize CIO functions in the federal government.

Congressional Oversight

A discussion of federal organization would be incomplete without considering congressional oversight. The fragmentation of oversight complicates efforts to improve homeland security, and cybersecurity shares in this problem. DHS has far too many oversight committees—more than 80—exercising jurisdiction, and we discussed whether to recommend streamlining congressional jurisdiction. Neither the rules of the House nor the Senate explicitly task committees with jurisdiction over cybersecurity. Some committees have taken up specific aspects of cybersecurity—including examining and legislating efforts in law enforcement and defensive capabilities—the absence of specific jurisdictional tasking from congressional leadership limits congressional oversight. Without rules changes that provide clear jurisdiction, responsibility for investigation, oversight, and policy development in cybersecurity will depend largely on member interest and the ability of committees to coordinate with each other.

We decided against making any recommendation on jurisdiction, however. Although we believe that it is important to streamline congressional jurisdiction over cybersecurity and homeland security, we also recognize that such a responsibility lies not with the next president, but with the Speaker of the House and the majority leader of the Senate. The president could engage these leaders in a discussion to streamline jurisdiction; but jurisdictional consolidation would not produce the immediate improvement in cybersecurity that our other recommendations offer. We believe that the next administration will achieve more lasting success by presenting a comprehensive package of cybersecurity improvements to the various committees; pragmatically, it is better that the next administration spend its time on achieving these goals rather than taking on jurisdictional battles in Congress.

3
Rebuilding Partnership with the Private Sector

Recommendation

- The U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities. We recommend the president direct the creation of three new groups for partnership that provide the basis for both trust and action:

  – A presidential advisory committee organized under the Federal Advisory Committee Act (FACA), with senior representatives from the key cyber infrastructures. This new body would incorporate the National Security and Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC);

  – A town-hall style national stakeholders' organization that provides a platform for education and discussion; and

  – A new operational organization, the Center for Cybersecurity Operations (CCSO), where public- and private-sector entities can collaborate and share information on critical cybersecurity in a trusted environment.

Securing cyberspace requires government and the private sector to work together. The private sector designs, deploys, and maintains much of the nation's critical infrastructure. This is important because unlike certain other elements of national security, cyberspace cannot be secured by the government alone. There is a bifurcation of responsibility (the government must protect national security) and control (it does not manage the asset or provide the function that must be protected).

Despite broad recognition of the need for partnership, government and the private sector have taken separate paths. Indeed, the so-called public-private partnership as it now exists is marked by serious shortcomings. This includes a lack of agreement on roles and responsibilities, an obsession with information sharing for its own sake, and the creation of new public-private groups each time a problem arises without any effort to eliminate redundancy.[17] As a result, the United States has a perplexing array of advisory groups with overlapping interests, inadequate resources, varying capabilities, and a lack of clarity around

[17] We do not question the value for private industry of the legal protections provided by the Critical Infrastructure Information Act of 2002.

roles and responsibilities. To achieve real partnership, we must simplify mission and organizational structure.

In many interviews, we found almost universal recognition that the status quo is not meeting the needs of either the government or the private sector with respect to trust and operational collaboration. This is the result of several factors. First, there is no clear vision regarding what needs to be accomplished. Second, there is not clearly articulated strategic initiative to guide private-sector efforts; indeed, even the recent cyber initiative was highly classified and largely kept from public discussion. Third, there is a lack of continuity in personnel in the government sector, including in the leadership ranks. Fourth, the government seems to believe it must share with everyone or no one, and because sharing with everyone poses risks for both companies and government, the exchange of information is constrained and awkward. Fifth, there are the usual issues related to a fragmented government that does not speak with a single voice or act as a unified entity.

Another problem for securing cyberspace is a diffusion of effort. Currently DHS identifies 18 different sectors as critical. This reflects a desire to be inclusive and a reluctance to tell sectors (and their congressional advocates) that they are not critical. For us, critical means that, if the function or service is disrupted, there is immediate and serious damage to key national functions such as U.S. military capabilities or economic performance. It does not mean slow erosion or annoying disruptions. Airliners demonstrate criticality. Having a video system or even bathrooms fail is annoying; having the engines or flight control systems fail is critical.

As the old military axiom has it: "He who defends everything defends nothing." To focus the defense of cyberspace, we have identified four critical cyber infrastructures: energy, finance, the converging information technology and communications sectors,[18] and government services (including state and municipal governments). This is not to suggest that all these sectors are identical. If power fails, the cascading effect is immediate and significant; by contrast, the result of an attack on government will depend upon what government service is affected. But these four sectors are all critical from a national security perspective, especially if that term correctly includes economic security. They form the backbone of cyberspace. We recognize that other sectors depend on cyberspace for their operations, but if their networks are damaged, not all of cyberspace is

[18] Outside the United States, this is referred to as the ICT sector. See "Telecommunications Task Group Final Report," CSIS Cybersecurity Commission, http://www.csis.org/media/csis/pubs/081028_telecomm_task_group.pdf, for more information on why "the boundary between information, information technology, and telecommunications services has become almost indistinguishable."

disrupted; they are not critical for its operation. Keep these sectors running, and cyberspace will continue to deliver services in a crisis. Bring them down and all other sectors will be damaged.

These critical cyber sectors are large, interconnected national networks that are the most vulnerable to broad disruption by cyber attack. Other infrastructures are more dispersed and less connected; penetrating and disrupting the water supply of one large city, for example, will not disrupt water supplies elsewhere. If these three networks, along with government services, can continue to operate in the face of attack, the nation can persevere in cyberspace. If they are crippled, online activities will come to an abrupt halt. These sectors are the focus of a new, simplified public-private partnership for cybersecurity.

We recommend concentrating on two key problems: how to build trust between the government and company executives and how to focus efforts on what is truly critical for cyberspace. Our essential recommendation for partnership is to simplify the structure and focus on building trust relationships between the private sector and the government. Information sharing, which drove much of the original thinking about how to work with the private sector, should become a tool, not a primary goal. The primary goal of the new partnership organizations should be to build action-oriented relationships rather than to share information that is either already available or that companies are reluctant to provide. This can be done by creating a simplified structure that has three parts: a new presidential advisory committee that connects the White House to the private-sector entities most important for cyberspace; a national town-hall organization that provides a dialogue for education and discussion, and a new operational organization.

The intent behind the three groups is to provide an inclusive platform for national engagement, something the United States currently lacks. The presidential committee lays the foundation for relationships with senior company executives who can provide advice and take action. (One rule for membership should be that executives without line responsibilities should not participate.) The town-hall group reaches audiences outside of the Beltway and the technology community. The CCSO provides a forum for operational collaboration.

Trust is the foundation of a successful partnership between government and the private sector. In the past few years, despite good intentions on both sides, our interviews found that trust between government and the private sector has declined. Trust is built on personal relationships and in small groups. Large, diffuse groups with a floating population are not conducive to building trust. Trust is also damaged when senior officials from government agencies do not cultivate it and when government plans and processes are opaque or inadequate. A senior-level FACA body would provide the foundation for rebuilding trust.

The President's Committee for Secure Cyberspace would absorb the National Security and Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC). It must be limited to C-level membership (not Washington representatives). We suggest that members not be allowed to send stand-ins and that the government always provides an appropriate senior official, such as the assistant to the president for cyberspace. Membership would be drawn from the leading companies in the critical cyber infrastructures. The President's Export Council is a useful precedent for the design of this new group.[19]

This recommendation comes from extensive discussion with members of existing groups, federal officials, and with officials of the UK's Center for the Protection of National Infrastructure. These discussions suggested that the existing advisory structure has failed in key areas. Existing groups do not provide the relationships with a go-to person in industry, someone who the president, the new assistant for cyberspace, or a cabinet secretary can call in a crisis for assistance. What we need is a group of executives from critical cyber infrastructure companies who will interact regularly with senior federal officials in order to create the trust relationships needed for real information exchange and for collaboration in a time of need.

We recommend that this new C-level group operate under FACA. Although some object that FACA stifles the ability to freely exchange information, our view is that this is more an issue of finding legal solutions that help the government comply with FACA but still have effective committees. FACA restricts the advice the federal government receives, less because of its actual meaning and more because of an overly broad interpretation. As interpreted by DHS, FACA has been used to restrict even operational collaboration with the private sector. Misinterpretation of FACA produces a process that is either overly inclusive (including entities without real stakes in the issue) or overly formal. This is a management problem, not a serious obstacle to discussion. One can comply with FACA and still get useful advice, but it takes work, focus, and commitment.

---

[19] The President's Export Council advises the president on policies and programs that affect U.S. trade performance. It provides a forum for discussing and resolving trade-related problems. The president appoints 28 private-sector members of the council. The council has an executive committee and creates subcommittees according to the council's interests. The President's Export Council meets at least twice each year, usually in Washington. The council's subcommittees may also hold meetings. President's Export Council members do not receive compensation for their service on the council. The council reports to the president through the secretary of commerce. The under secretary of commerce for international trade serves as the council's executive director. See http://www.ita.doc.gov/td/pec/index.html. PCAST, the President's Council of Advisors on Science and Technology, is another model although PCAST's membership is too academic for the more active role we envision.

The question of what to do with the existing advisory bodies is a difficult one. Our recommendation is to prune where possible. The Information Sharing and Analysis Centers (ISACs) for sectors critical for cyberspace (which are among the most effective) could become working groups attached to the new C-level body or the CCSO. These are the ISACs for the financial sector, the IT sector, and the multistate governmental ISAC. To the extent that the other ISACs and Sector Coordinating Committees provide value to DHS in its critical infrastructure protection mission, DHS should have the discretion to continue to work with them.

National Town-Hall Group

Our second recommendation, the creation of a new town-hall process, provides a vehicle to involve a broad range of stakeholders.[20] The town-hall meetings held as part of the process of developing the 2003 national cybersecurity strategy attracted large audiences and provided broad exposure to public concerns and government thinking. This new group would be inclusive and provide a platform for general messaging, information sharing, and stakeholder input. It would include companies and associations in the 18 sectors DHS identifies as critical, other industries, consumer groups, and trade associations. Its goal would be to build public awareness through town-hall meetings and to create opportunities for new relationships. The new process could work with existing broad-based groups, such as the FBI's Infraguard, the National Cybersecurity Alliance, or some of DHS's advisory groups. Absent the creation of this group, we will continue to rely on ad hoc and incomplete efforts to educate the public on how to operate more securely in cyberspace.

Center for Cybersecurity Operations

Finally, we recommend the creation of a new organization to address operational issues. We call this the Center for Cybersecurity Operations (CCSO), a new nonprofit organization where public- and private-sector entities can collaborate and share information on critical cybersecurity matters in a trusted environment. The CCSO would be guided by a board of directors consisting of cybersecurity leaders from government, industry, and academia.

The mission of the CCSO will be to address operational issues that affect critical cyber infrastructure. The CCSO can provide a transformation from a traditional government-centric partnership regime to one that would be an independent organization—a joint venture between government and private

[20] A town-hall meeting is a public meeting where all interested persons in a community are invited to attend, voice opinions, and hear responses from officials.

industry dedicated to protecting critical systems nationwide. The CCSO would be a self-governing organization. To ensure close collaboration with the overall national effort, we recommend that the new NOC have an ex officio seat on the CCSO's board of directors.

The CCSO would include a full-time, cross-sector operations center jointly manned by government and industry. The operations center would have a round-the-clock watch, which CCSO could bring to full strength during emergencies. It would form the core of an organization that can address important issues such as a widespread protocol vulnerability that can affect large numbers of vendors and users. The ISACs for sectors critical to cyberspace (the financial sector ISAC, the IT sector ISAC, and the multistate government ISAC) should become affinity groups attached to the CCSO. The CCSO would also develop new communities of interest, as needed, to address specific problems. For example, the CCSO could take a reported issue, identify affected entities, determine if there is a sizable community of interest, and then bring it together to help mitigate the issue or identify the right organization to do so.

The CCSO would work with other organizations that cover sectors that have a significant interest in cybersecurity issues. It would work with the academic community to analyze current and emerging problems, and it would foster the transfer of technologies from research to the market to help increase security. Additionally, the CCSO could manage the national stakeholders' forum recommended above and provide a venue for international cooperation among private-sector entities.

The success of this new organization is predicated on the federal government's willingness to utilize current and new organizations that provide value in the effort to protect cyberspace. The goal is a trusted and operationally focused collaborative alliance among the government, academia, and the private sector.

4
Regulate for Cybersecurity

Recommendations

- The president should task the NOC to work with appropriate regulatory agencies to develop and issue standards and guidance for securing critical cyber infrastructure, which those agencies would then apply in their own regulations.

- The NOC should work with the appropriate regulatory agencies and with the National Institute of Standards and Technology (NIST) to develop regulations for industrial control systems (ICS). This could include establishing standard certification metrics and enforceable standards. The government could reinforce regulation by making the development of secure control systems an element of any economic stimulus package that invested in infrastructure improvements.

- The NOC should immediately determine the extent to which government-owned critical infrastructures are secure from cyber attack, and work with the appropriate agencies to secure these infrastructures.

- The president should direct the NOC and the federal Chief Information Officers Council,[21] working with industry, to develop and implement security guidelines for the procurement of IT products (with software as the first priority).

- The president should task the National Security Agency (NSA) and NIST, working with international partners, to reform the National Information Assurance Partnership (NIAP).

- The president should take steps to increase the use of secure Internet protocols. The president should direct OMB and the NOC to develop mandatory requirements for agencies to contract only with telecommunications carriers that use secure Internet protocols. As part of its larger international strategy, the United States should work with like-minded nations and with the ITU and other bodies to expand the use of secure protocols.

[21] Chief Information Officers Council, http://www.cio.gov/.

It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives. The reason for this is that those who participate in the marketplace are necessarily constrained by economic forces: they must make a product priced low enough to be successful, they must meet the demands of a wide range of customers (not just governments), and they must ensure profitability. In this environment, companies have little incentive to spend on national defense, as they cannot fully recover their costs.

The role of regulation in cybersecurity has been contested since the drafting in 2003 of the first National Strategy to Secure Cyberspace. That strategy stated that "federal regulation will not become a primary means of securing cyberspace" and that "the market will provide the major impetus." In pursuing the laudable goal of avoiding overregulation, the strategy essentially abandoned cyber defense to ad hoc market forces. We believe it is time to change this. In no other area of national security do we depend on private, voluntary efforts. Companies have little incentive to spend on national defense as they bear all of the cost but do not reap all of the return. National defense is a public good. We should not expect companies, which must earn a profit to survive, to supply this public good in adequate amounts.[22]

We believe that cyberspace cannot be secured without regulation. The intent of such regulation is to increase transparency and improve resiliency and reliability in the delivery of services critical to cyberspace. We propose four sets of regulations: (a) the development of shared standards and best practices for cybersecurity in the three critical cyber-infrastructure sectors (ICT, finance, and energy) to improve performance and increase transparency, (b) the creation of new regulations that apply to supervisory control and data acquisition (SCADA) and other ICSs, (c) changes to federal acquisitions rules to drive security in products and services, (d) mandatory authentication of identity using robust credentials for critical infrastructure sectors (discussed in chapter 5). A reasonable, risk-based approach[23] would allow the government to prioritize categories of risk to cyber infrastructure and then design and implement proportionate measures to mitigate those risks.

The next administration should revisit the issue of regulation for cybersecurity and make two significant changes. First, industry and government should identify the level of security that markets will naturally provide. Regulation would create processes to fill the gap between what markets will

---

[22] A public good provides benefits to an entire society with very little incentive for any one person to pay for it.

[23] A risk-based approach assesses the likelihood and consequences of a particular category of event and prioritizes threats and responses based on that analysis.

naturally provide and what national security requires. The government's tool kit for this change should be viewed as expansive and flexible, including the use of policy and economic incentives to reinforce or supplant regulation.

We also reject the oft-heard argument that "voluntary regulation" provides the right solution. The central problem with voluntary regulation is that companies can choose when to adhere. Some companies will take a minimalist approach. Others will opt out when business conditions make opting out attractive. Weakness in compliance and enforcement makes voluntary regulation inadequate. In contrast, the dilemma with traditional regulation is inflexibility and prescriptiveness. Regulations change slowly. Prescriptive regulations that lay out exactly what companies must do meet a public goal not only risk becoming outmoded, they also risk stifling innovation; people will not look for more efficient solutions to a problem if they are required to rigidly follow a set practice.

We also are conscious, however, of the concerns raised by regulatory regimes. The dilemma with regulatory regimes is that they tend to be inflexible and difficult to change, particularly problematic traits in a rapidly changing world. Other concerns are that regulatory regimes may be overbroad (affecting more than necessary), underinclusive (affecting fewer than necessary), costly, and of arguable effectiveness. In emerging areas where innovation is crucial, there is also the concern that prescriptive regulations risk stifling innovation and discouraging the search for more innovative and effective solutions. Although these concerns are legitimate, we believe that a new regulatory model can address these concerns, significantly increase the state of cybersecurity, and make an indispensible contribution to the protection of national security.

To get the right regulations, we focus on two key points: the objective of any regulation, and how it is developed. Consistent with national security needs, the intent of any regulatory regime should be to improve security, transparency, reliability, and resiliency. This is important because some attacks can be prevented but some cannot, and, in the latter case, it is important that response and reconstitution of critical infrastructures happen quickly.

Our conclusion is that a new approach to regulation would better serve the public interest. The U.S. response to the Y2K experience suggests what this new approach could look like, one where a cooperative relationship between government and the private sector would replace command and control. The Y2K had two elements: The first was a government effort to educate, to cooperate in developing responses, and to lead by example. The second was a government mandate, through Securities and Exchange Commission (SEC) regulations, for publicly traded companies to report on the steps they had taken to secure their networks and their operations from disruption. In retrospect, this SEC requirement was as important as anything else in getting companies to put safeguards in place.

Y2K was a new model for government intervention, and the key to its success was that this model blended voluntary action with regulation.

Regulations will let the government hold critical cyber infrastructure to an adequate standard for security. Neither the market nor overly prescriptive, command-and-control regulation will produce this outcome. A new approach would combine the flexibility of the private sector in identifying best practices with the enforcement strength of the government in ensuring compliance. In this model, the existing regulatory agencies for telecommunications, finance, and energy would oversee a consultative process during which their industries would establish best practices for cybersecurity suited to their field. The agencies would embed these best practices in a regulatory and compliance framework and ensure that companies meet them. Government should set goals; industry should determine how best to accomplish these goals. Government should then ensure compliance.

The still developing relationship between North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC) demonstrates how this kind of regulation could work. Under the framework established by the Federal Power Act, the electric reliability organization (currently NERC) is responsible for proposing, for the review and approval of the FERC, reliability standards for the electric grid. These standards are statutorily defined to include "cybersecurity protection." FERC, upon its own motion or upon complaint, may direct the NERC to submit a proposed standard or modification on a specific matter. FERC can approve reliability standards or modifications proposed by NERC if it finds them in the public interest. If FERC disapproves a proposed standard or modification, it must remand it to the NERC for further consideration, beginning the standards review process again.

After the standards enter into effect, the NERC monitors compliance. It can direct violators to comply with the standards and impose penalties for violations, subject to review by, and appeal to, the FERC. FERC also may initiate enforcement on its own motion but, for most violations, will only review NERC enforcement actions. The current reliability standards have a three-year implementation plan that includes a timeline and milestones that identify when a responsible entity must begin work and be substantially compliant, in compliance, and auditably compliant with certain critical infrastructure protection reliability standards requirements. Certain entities must be "auditably compliant" with specific requirements in 2009 or 2010. The NERC-FERC model is not perfect,

and the regulatory authorities of FERC will need to be strengthened to adequately ensure security.[24]

Private companies and public organizations that own, control, operate, or maintain critical public infrastructure are in the best position to establish, adopt, and implement cybersecurity measures appropriate to their industry. Industry-specific security standards will promote a more effective national security posture by leveraging skills and subject-matter expertise within the affected industries to implement appropriate controls. Increased transparency and collaboration in these measures and increased federal oversight to ensure compliance combine the strengths of the public and private sectors.

Regulation is not a panacea and, if improperly implemented, can actually make matters worse by creating a false sense of security and creating incentives for the wrong behaviors (FISMA, for example, as currently drafted, creates incentives for document reviews rather for improving network security). But we think the next administration should apply the reinforced NERC-FERC model to other sectors. Beginning with existing best practices and standards for cybersecurity, the government could apply a regulatory requirement to secure networks adequately and oversee compliance with those new requirements. The standards would tell agencies and companies what outcomes they must achieve for cybersecurity but leave it to them to develop the best way to do this.[25]

This is where the NOC can play an important role, one that no agency currently plays. Our belief is that the NOC should provide oversight and coordination among regulatory agencies when it comes to cybersecurity, and the NOC could call attention to situations where regulation was inadequate. It would work with the regulatory agencies to issue standards and guidance defining adequacy in cybersecurity. It could assess both the adequacy of cybersecurity regulations and their implementation. It would review cybersecurity regulations to increase transparency and harmonization among cyber regulations and regulatory agencies so that companies that work across sectors would not be subject to conflicting regulatory regimes. As part of this task, the NOC would assume the Clinger-Cohen authorities currently exercised by OMB for "standards, guidelines, and associated methods and techniques for computer systems."

We considered whether to recommend assigning the authority to regulate cyber infrastructure to the NOC or DHS. We decided that it would be best to capitalize on the existing relationships and knowledge found in agencies like the

---

[24] There is an legislative effort to create a statuary mechanism within the Federal Power Act to grant FERC emergency authority to order temporary, interim cyber-security standards to protect against threats to national security.

[25] In addition to the Common Criteria are the ISO 9000 series, ISO 19779, SAS 70, FISMA, and NSTISSP 11.

Federal Deposit Insurance Corporation (FDIC) and the Nuclear Regulatory Commission (NRC). Under this federated approach, the NOC would ensure coordination by establishing benchmarks and thresholds for regulations (in other words, it would set the goals for cybersecurity), but each agency would retain the freedom to devise regulations in cooperation with their "clients" that meet these benchmarks and thresholds in the manner it considered best. In turn, the NOC would review the effectiveness of each agency's regulatory effort. Regulatory agencies for the critical cyber infrastructures would need to demonstrate to the NOC that their rules effectively protected against known vulnerabilities, attacks, and exploitations. Working with these agencies, the NOC should develop regulations immediately for critical cyber infrastructures. Over time, those regulatory standards for cybersecurity could be extended to other regulated sectors if this seemed useful.

The NOC would not have the authority to direct an independent regulatory agency to change its regulations, but if it judged them inadequate (or if an agency refused to provide information), it could call the inadequacy to the attention of the president. This practice has worked well for other national security matters, such as in the telecommunications arena. The presidential directive establishing the NOC should include a requirement for the appropriate regulatory agencies to report to the NOC and for the NOC to report to the president annually on the status and adequacy of agencies' cyber regulations.

SCADA and Industrial Control Systems

One important and atypical area for cyberspace regulation involves industrial control systems (ICSs), including supervisory control and data acquisition (SCADA) systems, that enable operators to monitor and control processes and even facilities from a centralized location or even automate processes that do not need constant human supervision. Although these systems are subject to many of the same concerns as other IT systems (vulnerabilities and configuration issues), the fact is that SCADA systems are designed to remain in place for very long periods of time and are often more difficult to upgrade. Initially, this was not a concern, as these systems were also not connected to the global Internet. But, over time, they are increasingly connected as people seek to take advantage of the benefits of connectivity. Thus, throughout our critical infrastructures, the command system rooted in cyberspace is at risk.[26]

[26] These systems include distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLC), and devices such as remote telemetry units (RTU), smart meters, and intelligent field instruments including remotely programmable valves and intelligent electronic relays.

We believe that current efforts to secure these critical systems are unfocused and do not specifically target the unique aspects of ICS.[27] The environment for ICS cybersecurity is similar to mainstream IT security 15 years ago—in a formative stage. Changing this will require many actions, including education, standards setting, and research. We believe that some regulation will be necessary.[28]

A national economic stimulus package that invests in infrastructure offers an opportunity to reinforce regulation and achieve needed cybersecurity improvements in control system and automation technology. The government could, as part of the stimulus, fund development programs with industry to create secure control system technology. This could be a multiyear effort, but by committing to buy and use these secure control systems products at federal power authorities and federal government-owned and -operated industrial activities, we could create incentives for the development of secure ICS.

Use Acquisitions to Increase Cybersecurity

Federal acquisitions rules provide another mechanism for the government to shape private-sector behavior. We recommend that the federal government require that the IT products it buys be securely configured when they are delivered. Currently most vendors deliver software with a very wide set of features and functions enabled, including some that can result in less secure operations if not properly configured by the purchaser. As software systems become increasingly complex, however, the difficulty of securely configuring these systems and maintaining those secure configurations has become a major technical and operational challenge. It is a challenge that can be solved by partnership between the government and industry.

Agencies have struggled with properly configuring software products. Analysis by the U.S. Air Force in 2002–2003 determined that configuring software products for security was expensive and often produced new vulnerabilities. NSA found that inappropriate or incorrect security configurations (most often caused by configuration errors at the local base level) were responsible for 80 percent of Air Force vulnerabilities. The Air Force assessed that it was spending far more to ensure that software was securely configured and to patch software defects than it was spending to purchase the products.

---

[27] See Dana A. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat," Report no. RL31534 (Washington, D.C.: Congressional Research Service, 2003).

[28] These regulations could include establishing standard certification metrics (for processes, systems, and personnel) and developing enforceable standards and their associated requirements (such as requiring senior officials in publicly traded companies to affirm that adequate measures have been taken to secure control systems).

To solve this problem, government and industry must engage on developing preconfigured security features for the federal marketplace designed for user needs and capabilities. We can use federal IT procurements to ensure that systems and software acquired by the government come securely configured from the vendor and that security is incorporated into products from the start of the design and development process. Government can use its procurement process to require that providers of IT products and systems are accountable and to certify that they have adhered to security and configuration guidelines. A further objective would be to examine the usefulness of open standards for addressing IT security problems in ways that both public- and private-sector organizations can implement. The most important benefit will be products that provide significantly improved security for federal systems as well as private-sector organizations that adopt this approach to procurement.

One precedent for this recommendation is the Federal Desktop Core Configuration (FDCC), an element of the CNCI. The FDCC is an OMB mandate that requires all federal agencies to standardize the configuration of settings on operating systems and for applications that run on those systems. The FDCC is aimed at strengthening federal IT security by reducing opportunities for hackers to access and exploit government computer systems. Although the FDCC had implementation problems—the speed at which it was put in place left insufficient time for consultation (and in OMB's defense, some consultations in Washington can drag on for years)—we believe that the FDCC effort should be continued and expanded.

The federal government, taken as a single organization, is the largest buyer of most information technology products. A carefully crafted acquisitions regime, combined with an expanded FDCC initiative could help drive the market toward more secure configurations. These steps will create a market for IT vendors using a variety of development methods to deliver.[29] The secure configurations mandated by the federal government and produced in this collaboration with industry would be available for use by state and local government organizations as well as the private sector. A collaborative effort between government and industry to resolve software vulnerabilities and to deliver secure products could result in lower overall costs over the life of a system, even if secure configurations initially resulted in a higher price.

Cooperation with the private sector in this area will be essential for success. Experience from similar initiatives has shown that coordination from the start with vendors with broad product bases within the federal government is essential.

[29] Methods include different software development models and hosted, or "cloud," computing deployment.

Government and industry partnerships can produce major improvements in security and can be built quickly. Security guidelines should leverage a number of existing and ongoing private-public collaboration efforts with broad industry and government participation.[30] These and other collaborative efforts have demonstrated that it is possible to develop security benchmark guidelines (sometimes referred to as security standards or configuration benchmarks) for software products.

Governance of security standards requires careful attention. To oversee the development and implementation of the security guidelines, we recommend that the NOC and OMB use the Chief Information Officers Council to undertake the development of standard security guidelines, settings, or specifications and to coordinate incorporation of those guidelines, settings, and specifications into government-wide contracting strategies (Smart Buy, GSA schedule, and Federal Acquisition Regulation, for example).[31] Once developed, the NOC and the Chief Information Officers Council can refer the guidelines and standards to appropriate policy and standards organizations for implementation.[32] These steps will ensure a level playing field for suppliers and support the broad adoption of the standards by stakeholders, including consumers in critical infrastructures and other private-sector industries.

While guidelines could be developed and implemented quickly for government procurements, full implementation may take longer owing to the complexity of enterprise software and the need to ensure that application of secure configurations do not disable critical services. Software should be the first priority, and software vendors would self-certify that they comply with the guidelines and that their products do not unlock the secure configurations of other products.

Configuration requirements can be reinforced by reforming the current practice for assessing security in hardware and software using the NIAP—a joint effort of NIST and NSA. Under NIAP, a set of NIST-accredited commercial laboratories assesses IT products according to agreed international standards known as the Common Criteria. The NIAP process requires extensive

---

[30] Public-private collaboration efforts include the Federal Desktop Core Configuration (FDCC), the SCADA Procurement Specifications, the BITS Product Certification Program, the Federal Energy Regulatory Commission (FERC) Reliability Standards for Cybersecurity, the National Information Assurance Partnership (NIAP) Common Criteria, as well as Product/System Certification Guides produced by NIST and the Center for Internet Security (CIS).

[31] One option would be to establish a Federal Cybersecurity Acquisition Governance Board under the auspices of the Chief Information Officers Council. This board could provide oversight for development of security guidelines, ensure broad coordination of the guidelines among industry organizations, and resolve issues that arise during the guideline development process.

[32] Such policy and standards organizations include OMB, NIST, ISO, the Institute of Electrical and Electronics Engineers.

documentation from the vendor for submission to an evaluation laboratory. The labs then engage in several months of analysis to validate vendor claims. Although the analysis provides assurance that the vendor claims are accurate, NIAP-validated products still contain vulnerabilities, and a higher rating does not necessarily guarantee a higher level of security. Further, there is no way to determine what happens when NIAP-reviewed products are all combined into a composite IT system.

Improving the NIAP process means moving from a post-facto review of documentation to processes that provide guidance and incentives to vendors to improve the security of their products in the design phase and in the methods for building secure IT systems from these products. Reform of NIAP should preserve the core attributes of NIAP, especially its acceptance as a standard by many of our allies and partners.

Today, Common Criteria is time-consuming and costly, and it focuses on assurances related to security features instead of to the security of the overall product being evaluated. We understand that the government is leading an effort to reform Common Criteria, and it might use an approach that looks at the development processes used by vendors to ensure that security is, in fact, part of the entire design-and-build process. We urge the government to complete this reform, in part because it will strengthen the security of products and in part because Common Criteria is used by many countries around the world. Reforming Common Criteria will not only improve cybersecurity in the United States but also improve cybersecurity in the larger global network of which the United States is a part.

Acquire Secure Internet Services

Federal acquisitions can drive the security of cyber services. Today's Internet evolved from research in the 1960s and 1970s. The fundamental protocols for the Internet (protocols are the rules governing how different devices connect to each other in cyberspace), which support connections between autonomous systems and domain name services, still reflect the design characteristics of the original concepts. These protocols were written for an earlier and more trusting era. Today's security approach is to overcome the vulnerabilities of the Internet by using a patchwork of niche products and work-arounds.

This is ineffective for providing the security necessary to protect the global Internet infrastructure from hackers, espionage, and criminal elements. We have seen, in the past few years, what appear to be tests of attacks to disrupt these backbone protocols in ways that would make the Internet unstable or unusable. Adoption of improved and more secure protocols has been slow because there is little or no demand for them in the market.

We found in our interviews that, although newer and more secure Internet technologies are available, the United States has lacked the incentives to adopt them. During the past decade, there have been significant efforts to design and prototype improved Internet protocols. More secure versions have been developed. While there is general agreement that more secure Internet protocols should be deployed, there has not been sufficient demand to lead Internet infrastructure providers to invest in them.

Federal acquisitions can remedy the lack of demand for secure protocols. Federal acquisitions can create incentives. The federal government is one of the largest purchasers of telecommunications services in the world. Federal acquisitions mandates could rapidly drive the market and provide benefits beyond the federal government. The United States can use this power as an incentive to move to a more secure Internet. Recommendations for accomplishing this follow in chapter 5.

5
Identity Management for Cybersecurity

Recommendations

- The United States should make strong authentication of identity, based on robust in-person proofing and thorough verification of devices, a mandatory requirement for critical cyber infrastructures (ICT, energy, finance, government services). The president should direct the NOC and appropriate agencies, using the federated regulatory model outlined in chapter 4 and consulting with industry and the privacy and civil liberties community, to implement critical infrastructure authentication. The president should receive a report on progress within six months.

- The United States should allow consumers to use strong government-issued credentials (or commercially issued credentials based on them) for online activities, consistent with protecting privacy and civil liberties.

- In a related initiative, the Federal Trade Commission (FTC; under its authority under Section 5 of the FTC Act or the Graham-Leach-Bliley Act) should implement regulations that protect consumers by preventing businesses and other services from requiring strong government-issued or commercially issued credentials for all online activities by requiring businesses to adopt a risk-based approach to credentialing.

- The president should, by the end of the first year of the presidential term, require every agency to report on how many of their employees, contractors, and grantees are using credentials that comply with HSPD-12 (Policy for a Common Identification Standard for Federal Employees and Contractors) and restrict bonuses or awards at agencies that have not fully complied.

A small community of researchers, many of whom knew each other, formed the original population of the Internet. In this community, confirmation of identity was not an issue. When the United States opened the Internet to commercial use, millions of poorly identified users flooded into cyberspace. As cyberspace expanded beyond the Internet to include many different networks and services, the ability to act anonymously shaped the new medium in ways both fortunate and unfortunate.

Anonymity is important (for the online expression of political views or for seeking of information about disease treatment, for example), but weak online identification is inappropriate in circumstances where all legitimate parties to a

transaction desire robust authentication of identity. In cases of online banking, for example, both the bank and the customer want to ensure that financial transactions are legitimate; in this context, weak authentication enables malicious behavior and crime without protecting any important societal value. Moreover, weak authentication can increase privacy risks when organizations attempt to confirm identity (when authenticating for online purchases, for example) by asking users to prove their identity by supplying more personally identifying information than would be needed if there were trustworthy credentials. Weak identification and authentication limit an organization's ability to enforce security policies to protect sensitive information and systems, and it hinders effective governmental and industry response to cyber attacks.

Creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy. Even sophisticated attackers face difficult challenges—and find their access restricted—because of better authentication. In the United States, the Federal Financial Institutions Examination Council's Guidance for Authentication in an Internet Banking Environment has spurred the use of stronger authentication in online banking. The experience of the DOD was that intrusion into DOD networks fell by more than 50 percent when it implemented Common Access Card. In light of experiences like this, we recommend that the United States adopt regulations that require robust authentication for access to critical infrastructures.

As part of an overall cybersecurity strategy, the government can accelerate the adoption of authentication. Many of the foundational pieces are already in place. For example, the federal government as well as state governments already issue various forms of identity documents based upon in-person proofing, from driver's licenses to passports. Such in-person proofing is critical because it greatly reduces the possibility that a criminal can masquerade as someone else simply by knowing some private details. HSPD-12 is another U.S. authentication initiative. It requires federal agencies to improve their identity and credentialing processes, using smart cards to secure both physical and logical access to federal facilities and networks. Although HSPD-12 has faced implementation problems, it and other federal initiatives offer the foundation for finally moving ahead in enabling authentication.[33]

Moreover, while government agencies issue identity documents for one purpose, the private sector often adopts those documents for other uses. Driver's licenses, Social Security numbers, and passports have all become de facto credentials used in commercial transactions. Explicitly allowing the commercial

[33] Four years after HSPD-12 was promulgated, OMB reported that only 29 percent of federal employees and contractors had received strong credentials; see http://www.whitehouse.gov/omb/pubpress/2008/103108_hspd12.html.

sector to use government-issued digital credentials for high-risk transactions (or to create their own robust commercial credentials)[34] could reduce fraud while increasing security and privacy. For example, an online merchant who suffers heavily from fraud could continue to sell to anyone but perhaps offer discounts or other incentives to those who use strong digital credentials. Most important, the use of digital identification reduces the need to authenticate people based upon personal, private details about themselves. Their use would mean we could reduce the transmittal, storage, and use of private information to identify individuals, thus increasing privacy and helping prevent crimes such as identity theft.

This requirement for improved digital credentials would be part of the regulations developed for critical cyber infrastructure sectors. Some sectors—finance, for example—have made considerable progress in improving authentication. Other sectors have not done as well. A basic principle for this regulatory approach is that unknown individuals or individuals using fraudulent identities should not be able to access critical infrastructure—the situation we find ourselves in currently.

A requirement for improved digital credentials is not confined to human actors. It is unavoidable that many interactions over public networks involve automated processes based on devices. The most important of these involve the numerous processes that control critical infrastructures, which rely entirely on automated systems. The need for these interactions to be properly authenticated is as important as the need for human authentication. Thus, authentication regulations must also address the need for device authentication so that interactions involving devices can also be trusted.

Past efforts to develop digital credentials suitable for transactions of varying levels of risk have failed for two reasons. First, there was no governance structure that let authentication systems "federate," so that one system could determine how much it could trust a credential issued by another. Second, the public perceives private credentials not firmly linked to government credentials or processes as inadequate for many transactions. Both of these problems require a solution that provides transparency, accountability, and protection for privacy and civil liberties.

Balancing Security and Civil Liberties

Any recommendation to improve authentication raises important privacy and civil liberties issues. While anonymity and weak authentication of identity create some of the greatest security challenges in cyberspace, they also serve to protect those

[34] A robust credential is one that is technically strong, firmly linked to an identity (by in-person proofing or the use of government-issued documents), and embedded in a transparent and accountable system.

who, for example, want to engage in unpopular speech. The question is whether we improve, for cybersecurity purposes, authentication while we protect other important social values such as privacy and free speech. We have concluded that security in cyberspace would benefit from stronger authentication and that the government must require strong authentication for access to critical infrastructure. In doing this, the United States must improve authentication in a balanced manner, with full protection of privacy and civil liberties.

Privacy and confidentiality are central values that any government cybersecurity initiative must respect. For authentication systems to be widely adopted, privacy concerns must be addressed. A new initiative can do this by making authentication requirements proportional to risk—high-risk situations require strong authentication, while the lowest-risk situations require no authentication.[35] The goal is to avoid a once-size-fits-all approach to credentialing. This could be done, for example, by providing an opt-in requirement for using such credentials and requiring businesses and other services to use a risk-based approach in determining the level of authentication required.

In addition, consumers should have choices about the authentication they use and be able to tailor the identity information they exchange to provide the minimum needed for a transaction. Allowing consumers to choose and to tailor the information they provide will enhance both security and privacy. Acceptance of stronger authentication can also be increased by implementing rules about the secondary use of information used for authentication purposes and ensuring the destruction of personally identifiable information when it is no longer needed. The United States should factor these concerns into the design and implementation of new requirements as well as in the modification of existing systems.

Our discussions made clear that government programs must provide security while also protecting privacy and civil liberties. As part of this, the United States will need to prohibit demands for robust credentials when people seek access to public government data. For commercial use outside of critical infrastructure, decisions on authentication should be left to consumers and commercial entities to choose the level of authentication if any is desirable and what credentials to use. Government must be careful not to inhibit or preclude anonymous transactions in cases where privacy is paramount (such as a person accessing a Web site to get information on a medical condition).

---

[35] A high-risk situation would be accessing critical infrastructure control network or system. A low risk activity would be a normal commercial activity (buying shoes) or other products) or accessing a website for informational purposes. NIST has defined four levels of authentication assurance, for example, that rank transactions by risk.
http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm

We recognize the sensitivity of any recommendation to improve authentication, but we also believe it is possible to improve authentication for critical functions while simultaneously preserving those liberties. For new authentication requirements to be optimally designed and implemented, development must at the beginning engage civil society and incorporate the appropriate protections for civil liberties and privacy.

6
Modernize Authorities

Recommendations

- The president should direct the Department of Justice to reexamine the statutes governing criminal investigations of online crime in order to increase clarity, speed investigations, and better protect privacy.

- In the interim, the attorney general should issue guidelines as to the circumstances and requirements for the use of law enforcement, military, or intelligence authorities in cyber incidents.

- The president should work with Congress to rewrite FISMA to use performance-based measurements of security.

- The president should propose legislation that eliminates the current legal distinction between the technical standards for national security systems and civilian agency systems and that adopts a risk-based approach to federal computer security. The NOC, working with OMB, NIST, and NSA, should develop risk-based standards covering all federal IT systems.

Cyberspace has evolved continuously and quickly since the early 1990s, and this rapid pace means that crucial authorities for better cybersecurity are increasingly outdated. As an indispensable part of reorganizing the federal government to meet the challenges of cyberspace, we believe that the next administration should work with Congress to revise the legal and budgetary authorities regulating the federal government's work in cybersecurity.

Law Enforcement Authorities

Although FISA has recently been revised, the criminal-law authorities governing the collection of electronic evidence have not. In particular, rules for law enforcement access to data held or transmitted by third parties deserve review. These rules (including the Wiretap Act, the Stored Communications Act, and the Pen Register and Trap and Trace Statute) have been written and amended over the course of 40 years, resulting in a complex interchange of definitions, prohibitions, and permissions. To the extent that the sheer weight of legal complexity deters or delays investigations or cooperation among the private sector and the government after a network attack or penetration, these current laws may damage the nation's cybersecurity.

Moreover, if current statutes are not aligned with the ways in which the public actually uses technology, they can invite confusion and litigation, fostering neither effective investigations nor individual privacy and civil liberties. Increasingly, people are remotely storing their sensitive information on services, such as Web mail and calendaring, and application of existing law to these new technologies is uncertain. A reexamination of these statutes should attempt to both speed law enforcement access in appropriate cases and strengthen privacy for legitimate users, and should consider ways in which social expectations of online privacy may be changing. The review should cover a full range of data, including content and transactional data and should consider whether particular legal thresholds should be raised or lowered. It will also be important to simplify the entire statutory structure, modernizing definitions and removing outmoded constructs and distinctions.

The reexamination may also reveal opportunities to update procedural-law processes to reflect modern investigative realities, including the nationwide, rapid nature of cyber investigations. For example, certain geographic or jurisdictional requirements for search warrants that were appropriate in the physical world may be increasingly impracticable in the online environment. Similarly, it may also be time to consider creating rules for remote online execution of a data warrant. This may be especially useful in investigations of terrorism, espionage, cyber crime, organized crime, or any other where there is a risk of data destruction or danger to the officer.

Finally, we appreciate that many may be concerned about where this review may lead. Law enforcement agencies may be concerned that the current rules, which they have learned to navigate, may become more stringent and an impediment to speed. Civil libertarians may worry that, in a world consumed with terrorism, the protection for civil liberties may take a back seat to national security and public safety. And U.S. companies may fear the spread of European-style data privacy rules that restrict commercial uses of data pertaining to individuals. These concerns are all legitimate. But in a world where the Internet citizen is about to embrace cloud computing (or, put another way, in a world where a citizen's most sensitive data may routinely be globally accessible and in the possession of third parties), we have a unique opportunity to proactively decide what the right rules should be. Otherwise, the inconsistencies in applying the old laws to a new paradigm could jeopardize all of these competing concerns.

Federal Information Security Management Act (FISMA)

One law is of particular importance to the government's use of information technology: the Federal Information Security Management Act, or FISMA. FISMA is in critical need of an overhaul. FISMA mandates yearly reports in

which agencies report to OMB on their efforts at information security and their compliance with various standards using OMB-defined metrics and reporting templates. These metrics and reports are compiled by OMB and submitted to Congress in an annual compliance report. FISMA also tasks NIST to develop standards and best practices for use by federal departments and agencies in assessing their compliance with FISMA and improving their overall IT security.

Passed in 2002 to bolster federal network security, FISMA strengthened provisions previously contained in the Government Information Security Reform Act that required federal agencies to identify and minimize potential risks in information systems for unclassified programs or functions. FISMA creates a governance framework for managing security investments and assessing the overall effectiveness of security programs. As such, FISMA requires OMB to review and approve, or disapprove, agency information security programs annually, and this process provides an important opportunity for OMB to take stock of agency programs and procurement requirements for security. The annual FISMA reports are intended to provide government executives an overall insight into the security management of the network. FISMA was not designed to provide minute-by-minute views into network security.

To some in government and industry, FISMA has become a paperwork exercise rather than an effective measure of network security. They cite examples where an agency can get good marks in FISMA and still be vulnerable. FISMA lacks effective guidance and standards for determining appropriate levels of risk; it lacks requirements for testing or measuring an agency's vulnerabilities or its plans for mitigating such vulnerabilities; it fails to define agency responsibilities for effective controls over contractors or vendors; and it does not recognize the emergence of new technologies and network architectures.

Current efforts to modernize FISMA include new provisions on network security monitoring that may greatly improve agency capabilities to address operational security issues and reduce exposure to rapidly emerging threats. A revised FISMA should require that agencies demonstrate that their systems are effectively protected against known vulnerabilities, attacks, and exploitations by using metrics informed by U.S. offense capabilities and by actual performance. A first step would be to reinforce the current FISMA compliance process at selected agencies with a periodic vulnerability scan and red-team attack assessment, perhaps conducted as training exercises by DOD cyber assets. Finally, the revision of FISMA should assign to the NOC the ability to use continuous monitoring (perhaps based on the Einstein program) of security and performance rather than an annual review of paper processes.

Civilian and National Security Systems

The historic distinction between civilian agency systems and national security systems no longer serves the U.S. interest. Civilian agencies have not received the technical assistance they need to protect their systems in the current threat environment.

The distinction between national security and nonnational security systems in federal information technology dates back to the Computer Security Act of 1987. Congress, in enacting the law, sought to avoid any potential chilling effect on the free flow of information between government and the citizenry, which might occur if a military agency oversaw security for civilian agency systems. The statutory framework that emerged from the act assigns responsibility for civilian agency networks to OMB and NIST, and for military and intelligence networks to DOD and NSA. There is only loose coordination between civil and national security even though these communities have become increasingly interconnected. Commission members were told of one instance when all federal systems came under attack, and DOD quickly developed countermeasures; but because of the civilian–national security split, civilian agencies did not find out about this until more than a month later.

A new approach would end the distinction between civilian and national security and instead assign responsibility according to the sensitivity of information. In this risk-based approach, agencies would assess the sensitivity of the information they hold on their networks—information whose loss would adversely affect the privacy of citizens, the operations of government, or U.S. economic interests. When agency activities involve sensitive information, they would implement more extensive protection in compliance with a risk-based approach, mandated by OMB and based on technical advice from NSA and NIST. Where agency missions dictate the need for open access and transparency, agency systems would allow easy access. Privacy could be protected by requiring privacy impact assessments and the application of fair information principles under the Privacy Act.[36]

[36] An example of this approach lies with OMB's 2003 policy on authentication in civilian agency networks, which was issued in consultation with DOD and NIST. This policy lays out four levels of assurance for authentication, where each level requires more stringent action by agencies on the basis of increasing risks and sensitivity. OMB's policy requires that agencies address privacy regardless of assurance level, and this principle was repeated as part of the issuance of HSPD-12.

7
Build for the Future

Recommendations

- The president should direct the NOC to work with the relevant agencies and the Office of Personnel Management to create training programs and career paths for the federal cyber workforce and to work with the National Science Foundation to develop national education programs.

- The NOC, working with the Office of Science and Technology Policy (OSTP), should provide overall coordination of cybersecurity research and development (R&D). As part of this, the United States should increase its investment in longer-term R&D designed to create a more secure cyber ecosystem.

As a nation, we are in the midst of a set of larger transformations—economic, political, and military—driven by the technology of cyberspace. We cannot predict the form these transformations will take, but we can begin to build national capabilities that will improve the ability of the United States to manage and benefit from them. The following recommendations—on education and research—address this transformation. They can be implemented quickly, but it will take time to see their return. This does not mean we can ignore them, however.

The story of air power illustrates this. Americans were the first to fly, but as a nation, we invested little or nothing in creating better aircraft or in training pilots. This failure reflected, at first, a failure to recognize that the nature of conflict had changed and that air would now be a new domain for warfare. Later, it reflected an unwillingness to invest or to recognize the scope of foreign threats our nation faced. The result was that the United States entered two world wars handicapped by its lack of investment in workforce and research in air power.

We hope not to face another world war, but that does not mean that the United States does not face conflict, challenge, and attack, particularly when it comes to cyberspace. Commission interviews and research show that currently, in cyberspace, the advantage lies with the attacker. These recommendations call for long-term investment in the workforce and the new technology that will remove that advantage.

Cyber Education and Workforce Development

The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the federal government. In other words, just as in the world wars, we have a shortage of "pilots" (and "ground crews" to support them) for cyberspace.

Why has the market not provided the skilled workforce we need? The shortfall reflects a larger decline in the science and technology workforce in the United States. Some students, seeing funding cuts for research, are reluctant to go into computer sciences. Others are deterred by the memory of the dot-com bust. The government competes with the private sector for these scarce skills, and one refrain Commission members heard was that skilled federal employees, seeing no clear path for promotion in government and ample rewards on the outside, are constantly tempted to jump ship.

We believe there are two remedies for these problems. The first is to increase the supply of skilled workers. This will benefit both government and the private sector. The second is to create a career path (including training and advancement) for cyberspace specialists in the federal government.[37]

Ideally, increasing the supply of skilled cyber workers would be part of a larger national effort to address the declining science and technology workforce. The model for this is the 1958 National Defense Education Act, which improved national security and strengthened the economy. A larger effort poses complex challenges, however, and a focused program that emphasizes cybersecurity will be easier to obtain. The simplest approach would be to expand the Scholarship for Service, a National Science Foundation scholarship program that provides tuition and stipends, and reinforce this by requiring accreditation of schools where scholarships are provided for computer security studies.

The United States must also develop a career path for cyber specialists in federal service. Creating this career path entails a number of steps, including minimum entry requirements for cyber positions, training in specialized security skills,[38] and a national cyber skills certification program. The Office of Personnel Management, working with key agencies engaged in cyber defense and offense, needs to establish rewarding career paths and advanced training. To manage workforce development, we recommend that the NOC create an interagency body

---

[37] Career path refers to the ability to move to more senior positions as experience is gained, without moving to different career fields, to be compensated according to increased skills, and to expect that a particular field will provide for continued training and advancement.

[38] Examples include vulnerability analysis, intrusion detection, digital forensics, reverse engineering, protocol analysis, penetration testing, secure network engineering, and computer network attack.

responsible for developing standards for skills and knowledge to meet cyber missions and functions.

This career path should transcend specific departments and agencies. We would model it on the Federal Law Enforcement Training Center (FLETC), which provides training to federal employees in the skills of law enforcement officers. The program should initially focus on national security–related missions (including critical infrastructure) but could later be expanded to other mission areas.

Further, existing federal training centers should begin to provide baseline cyber skills to all federal employees who pass through their programs. To ensure quality throughout the curricula, an accreditation body similar to the Federal Law Enforcement Training Accreditation or the Council on Occupational Education[39] needs to be established that will provide the oversight to guarantee that all federal training centers offering cyber training adhere to quality, effectiveness, and integrity standards.

In addition, the White House could work with Congress to introduce legislation that would allow the Office of Personnel Management to offer more flexibility in hiring and retaining the employees with specialized cyber skills. Civil service reform is far outside the scope of our report, but agencies must be able to attract skilled candidates, then hire and retain them using twenty-first-century methods such as flexible hiring authorities, recruitment and retention bonuses, increased growth opportunities, and student loan repayments.

This is a complicated series of steps, but the steps are necessary to produce the skills needed for cyberspace. Again, there is a precedent worth bearing in mind. Many Americans believe that our nation still leads in cyberspace, just as many Americans in 1957 believed the United States led in space until a Soviet satellite appeared over their heads. The Soviet satellite launch shook America's belief that our math, science, and engineering education programs were superior to those in all other countries. In 1958, we were able to respond quickly with educational programs to meet a new kind of security challenge. We believe that the same rapid response is required now for the challenge facing the United States in cyberspace.

Building a skilled workforce does not require constant presidential attention. A presidential directive must initiate the process, however, by identifying it as a goal and a priority for resources, by creating new interagency management structures, and by tasking the NOC and the relevant agencies to begin work and report on progress.

---

[39] See the Web sites of Federal Law Enforcement Training Accreditation at www.fleta.gov and the Council on Occupational Education at www.council.org.

Expand and Focus Research and Development for Cybersecurity

The federal government plans to spend about $143 billion in 2009 on R&D. We estimate that two-tenths of 1 percent of that will go to cybersecurity.[40]

To put this in context, the president's fiscal year 2009 budget requests $29.3 billion for life science research, $4.4 billion for earth and space science, $3.2 billion for the Advanced Energy Initiative, $2.0 billion for the Climate Change Science Program, and $1.5 billion for nanotechnology. The National Information Technology R&D (NITRD) programs will receive $3.5 billion. Cybersecurity R&D will receive about $300 million.[41]

Federal R&D funding is a politically complex issue. There are many worthy claimants, each of whom asserts that its field of research needs increased funding and should receive priority. Further, overall U.S. spending on R&D has been flat for many years (despite recent increases), making the competition for funding even more ferocious. But, given the importance of cybersecurity to all aspects of our national defense and economy coupled with the more sophisticated cyber threats we face, a $300 million R&D investment in cybersecurity is inadequate.[42]

The CNCI recognized the shortfall in cybersecurity-related R&D investment and made efforts to change this. The CNCI calls for increased R&D funding in the future, for both near-term improvements with current technology and longer-term efforts. The longer-term effort has two main goals: (1) constructing a national research and technology agenda that both identifies the most promising ideas and describes the strategy that brings those ideas to fruition and (2) jump-start multidisciplinary development efforts. A series of workshops will be held in 2009 to develop the submissions received; however, the outcome of this process is at best uncertain. NSF, Defense Advanced Research Projects Agency (DARPA), Homeland Security Advanced Research Projects Agency, and other agencies have issued similar calls in the past without effect. Also, the planned levels of funding for long-term research have not been published.

The next administration has a major opportunity to use R&D to improve cybersecurity. Research so far has been helpful and informative but too incremental in nature. The NITRD exists largely as a passive compilation of R&D activities by the NSF and various federal agencies rather than a driver of an aggressive research agenda. Ad hoc and uncoordinated investments by various

---

[40] "Federal R&D Funding by Budget Function: 2007–09: Detailed Statistical Tables, NSF 08-315," National Science Foundation, Division of Science Resources Statistics. September 2008, http://www.nsf.gov/statistics/nsf08315/.

[41] In addition to the $280 million reported by the NITRD, DHS has $19.5 million for FY 2009 in its Science and Technology Program for cybersecurity research, which is not included in the NITRD figures. Other pockets of funding not accounted for here may exist in other agencies.

[42] For identification of many major research topics, see "Hard Problem List," INFOSEC Research Council, November 2005, http://www.cyber.st.dhs.gov/docs/IRC_Hard_ Problem_List.pdf.

agencies have not provided the full return for security, and the Commission's view is that this will not change until strategic priorities for cybersecurity R&D are established. Closer integration of research efforts with the new strategy for cybersecurity would maximize benefits from increased investment. Just as DOD has successfully marshaled R&D to provide military advantage to the United States since the 1940s, the new governance structure must harness R&D to the cybersecurity needs of the United States.

One particular area for research involves metrics to assess the overall effectiveness of cybersecurity initiatives. A central part of judging whether a product or initiative has improved security is to develop the metrics that can measure progress, but we lack meaningful measures of security. As part of an expanded cyber research agenda, the NOC and the OSTP should make the development of meaningful cybersecurity metrics and better assessment tools a priority in the national research agenda. Research efforts should focus on the creation of metrics and tools that will allow system owners to measure risks and determine how best to minimize those risks through informed investment.

Perhaps the most important game-changing research involves what we call "rearchitecting the Internet." The Internet is a human creation and as a veteran of the 1970s DARPA effort said to us, "We built it; we can change it." Today's Internet operates with protocols written in the 1970s and 1980s. At that time, trust was not an issue. The Internet's creators assumed that users would not cause deliberate harm and that any issues would be caused by technical problems with computers or network components. Most of the current Internet stability and security issues exist because of the abuse of these older vulnerable technologies by intentionally malicious users. Updating the core protocols of the Internet to be more resilient against attack could make cyberspace an environment of greater security and trust. Research on how to make the Internet fundamentally more secure would provide global benefits for security and commerce.

Conclusion
Winning the Hidden Battle

Cybersecurity is among the most serious economic and national security challenges we face in the twenty-first century. Our investigations and interviews for this report made it clear we are in a long-term struggle with criminals, foreign intelligence agencies, militaries, and others with whom we are intimately and unavoidably connected through a global digital network; and this struggle does more real damage every day to the economic health and national security of the United States than any other threat. As one general officer put it in his briefing to us: "In cyberspace, the war has begun."

But the national challenge involves more than security. We believe that the next administration can improve the security situation in relatively short order. We will never be fully secure in cyberspace, but much can be done to reduce risk, increase resiliency, and gain new strengths. More important, the effort to improve cybersecurity offers the opportunity to rethink how the federal government operates and to build collaboration across organizational boundaries. Our goal should not be the best defense, but a federal government that can securely take full advantage of cyberspace.

Many of our interviews encouraged us to think of a holistic approach to cybersecurity, one that looked beyond security alone and asked how best to enable and assure essential services in cyberspace. The progression of our thinking led from an improved DHS to an expanded cybersecurity function in the NSC; from an expanded NSC to a new cybersecurity entity; and from a new cybersecurity entity to one that looked broadly at enabling the secure and reliable use of cyberspace for national functions. Whether we call this the transition to an information economy or simply note that services, intangible products, and digital connections will be increasingly important in driving e economic and social activity, our goal must be a government and nation attuned to the new environment technology has created and where the secure use of cyberspace creates new opportunities for collaboration, growth, and national advantage.

The start of a new administration always brings opportunities for change and improvement. It will be easy to be distracted, however, both by the larger crisis that the nation faces and by the discussion of cybersecurity itself. Many different communities—privacy, law enforcement, business and technology, and national security—bring differing and at times discordant views to the issue. We can turn this diversity into strength if we make the broad national interest the lodestar for our decisions. Finding ways to take better advantage of cyberspace will help give the United States a competitive edge in a world where we are currently running

behind our competitors. The next administration has an opportunity to improve the situation; we hope these recommendations can contribute to that effort and its success.

Appendix A
Commission Members

Chairs

Representative James R. Langevin
Chairman of the Homeland Security Subcommittee on Emerging Threats, Cyber Security and Science and Technology

Representative Michael T. McCaul
Ranking Member on the Subcommittee on Emerging Threats, Cyber Security and Science and Technology

Scott Charney
Corporate Vice President for Trustworthy Computing, Microsoft Corporation

Lt. General Harry Raduege, USAF (Ret.)
Chairman, Center for Network Innovation, Deloitte & Touche LLP

Commission Members

Peter Allor
Senior Security Strategist, Cyber Incident & Vulnerability Handling, PM, Office of the CTO, IBM Internet Security Systems

Michael Assante
Vice President and Chief Security Officer, North American Electric Reliability Corporation

Marjory S. Blumenthal
Associate Provost, Academic, Georgetown University; former Executive Director, Computer Science and Telecommunications Board, National Academies

Adam C. Bordes
Principal, Shamrock Government Relations, LLC; former Professional Staff Member, House Committee on Oversight and Government Reform

Scott Borg
Director and Chief Economist, U.S. Cyber Consequences Unit

Mason Brown
Director, SANS Institute

Paula J. Bruening
Deputy Executive Director and Senior Policy Adviser, the Centre for Information Policy Leadership, Hunton & Williams LLP

Frederick R. Chang
Associate Dean, College of Natural Sciences, University of Texas at Austin

Dan Chenok
Senior Vice President and General Manager, Civilian Agency Services Division, Pragmatics

Eric Cole
Chief Scientist and Senior Fellow, Lockheed Martin Corporation

Mary Ann Davidson
Chief Security Officer, Oracle Corporation

Jerry Dixon
Director of Analysis, Team Cymru; former Executive Director, NCSD, U.S. Department of Homeland Security

Edward Felten
Professor of Computer Science and Director of the Center for Information Technology Policy, Princeton University

Liesyl Franz
Vice President, Information Security Programs and Policy, Commercial Sector Group, Information Technology Association of America

Dan Geer
Principal, Geer Risk Services

John Gilligan
Principal, Gilligan Group, Inc.

Ed Giorgio
President and Cofounder, Ponte Technologies

Chris Hankin
Director, Federal Affairs, Sun Microsystems, Inc.

Jessica Herrera-Flanigan
Monument Policy Group; former Staff Director and General Counsel, House Committee on Homeland Security

Beryl A. Howell
Executive Managing Director and General Counsel, Stroz Friedberg LLC; former General Counsel to Senator Patrick Leahy, Chairman, U.S. Senate Committee on the Judiciary

Tom Kellermann
Vice President, Security Awareness, Core Security Technologies

Shannon Kellogg
Director of Information Security Policy, Office of Government Relations, EMC Corporation

Paul Kurtz
Partner, Good Harbor Consulting

Bruce McConnell
Independent Consultant

John Nagengast
Executive Director, Strategic Initiatives, AT&T Government Solutions

William Pelgrin
Director, New York State Office of Cyber Security and Critical Infrastructure Coordination

Greg Rattray
Principal, Delta Risk, LLC

Frank Reeder
President, Reeder Group; CIO counsel, OMB

Philip Reitinger
Chief Trustworthy Infrastructure Strategist, Microsoft Corporation

Randy V. Sabett
Partner, Sonnenschein Nath & Rosenthal LLP

Marcus Sachs
Executive Director for Government Affairs, National Security Policy, Verizon Communications; and Director, SANS Internet Storm Center

Phyllis A. Schneck
Vice President, Cyber Intelligence and Critical Infrastructure Protection, McAfee, Inc.; Founding Chairman and Chairman Emeritus, InfraGard National Members Alliance

Suzanne Spaulding
Principal, Bingham Consulting Group; former Assistant General Counsel, Central Intelligence Agency

Martha Stansell-Gamm
(Retired) Chief, Computer Crime and Intellectual Property Section, Department of Justice

John N. Stewart
Vice President and Chief Security Officer, Cisco Systems, Inc.

Michael Vatis
Partner, Steptoe & Johnson LLP, former Associate Deputy Attorney General; former Director, National Infrastructure Protection Center

Amit Yoran
Chairman and CEO, NetWitness Corp.; former Director, National Cyber Security Division and US-CERT

Marc J. Zwillinger
Chair, Internet, Communications & Data Protection Group, Sonnenschein Nath & Rosenthal LLP

Ex Officio Members

Sameer Bhalotra
Professional Staff Member, Senate Select Committee on Intelligence

Margie Gilbert
Senior Intelligence Service, Central Intelligence Agency

Kevin Gronberg
Senior Counsel to the House Committee on Homeland Security; Staff Lead, House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

R. Shawn Gunnarson
Senior Counsel, Office of Senator Robert F. Bennett

Erik Hopkins
Professional Staff Member, Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs

Alex Manning
Legislative Director, Office of Representative Michael McCaul

Douglas Maughan
Program Manager, Cyber Security R&D, Science and Technology Directorate

Jacob Olcott
Staff Director and Counsel, House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Greg Pinto
Director, Regulatory Coordination Office, U.S. Department of Homeland Security.

Tony Sager
Chief, Vulnerability Analysis and Operations Group, National Security Agency

Caryn Wagner
Former Budget Director, House Permanent Select Committee on Intelligence

Gregory C. Wilshusen
Director, Information Security Issues, Government Accountability Office

Senior Advisers

David L. Brant
Director, Deloitte Consulting LLP, Washington, DC

Guy L. Copeland
Vice President, Information Infrastructure Advisory Programs Special Assistant to the CEO CSC

Howard Schmidt
President and CEO, Information Security Forum

Orson Swindle
Senior Policy Adviser and Chair, Security Initiatives, Center for Information Policy Leadership at Hunton & Williams; former FTC Commissioner

Francis X. Taylor
Vice President and Chief Security Officer, The General Electric Company

William Vass
President and COO, Sun Microsystems Federal, Inc.

Appendix B
Expert Advisors to the Working Groups

Michael Aisenberg, Special Assistant and Counselor to the President, EWA Technologies

Rich Baich, Commanding Officer, U.S. Naval Reserve Navy Information Operations Command

John Biccum, Senior Security Strategist, Trustworthy Computing Group, Microsoft

Jeff Dagle, Chief Electrical Engineer, Pacific Northwest National Lab

Liesyl Franz, Vice President, Information Security Programs and Policy, Commercial Sector Group, Information Technology Association of America

Gerald Freese, Director, IT Engineering Security, American Electric Power

Sy Goodman, Professor of International Affairs and Computing, Georgia Institute of Technology

Jim Gosler, Senior Scientist, Sandia National Laboratories, U.S. Energy Department

Les Guice, Vice President for Research and Development, Louisiana Tech University

Tom Harper, Director, CI Cyber Program, U.S. Department of Energy

Dan Hickey, DOD IA/CND Solutions Architect, McAfee, Inc.

Katie Ignaszewski, Governmental Programs Executive, Security, IBM

Jeff Kimmelman, CTO and Principal Architect, Network & Security Technologies, Inc.

Clint Kreitner, President and Chief Executive Officer, Center for Internet Security

Herbert Lin, Senior Scientist, National Research Council

Paul Nicholas, Principal Security Strategist, Microsoft

Mike Peters, Energy Infrastructure & Cyber Security Adviser, Federal Energy Regulatory Commission

Tim Roxey, Technical Assistant to Vice Chairman Constellation Energy—Security;

Deputy Chair, Nuclear Sector Coordinating Council

Tim Sheehy, Director of Electronic Commerce, IBM

Gregory B. White, Director, Center for Infrastructure Assurance and Security, The University of Texas at San Antonio

Jeffrey H. Wright, Director, Koniag Services Inc.

Appendix C
List of Briefings

November 13, 2008	Closed briefing. Marie O'Neill Sciarrone Special Assistant to the President and Senior Director for Cybersecurity and Information Sharing Policy, Homeland Security Council, White House
November 10, 2008	Closed briefing on the P12 Initiative. Rear Admiral Michael A. Brown (USN) Deputy Assistant Secretary for Cyber Security and Communications, National Protection and Programs Directorate, Department of Homeland Security
November 6, 2008	Closed briefing. Department of Defense Cyber Crime Center Colonel Steven D. Shirley (USAF) Executive Director of the Department of Defense Cyber Crime Center
October 17, 2008	Closed briefing. Robert D. Jamison Under Secretary for the National Protection and Programs; Director, Department of Homeland Security
October 6, 2008	Closed briefing. Karen S. Evans Administrator of e-Government and Information Technology, Office of Management and Budget
September 25, 2008	Closed briefing. Rear Admiral Michael A. Brown (USN) Deputy Assistant Secretary for Cyber Security and Communications, National Protection and Programs Directorate, Department of Homeland Security
September 18, 2008	Public event: Federal Responses to Cybersecurity. Melissa Hathaway Senior Adviser to the Director of National Intelligence and Cyber Coordination Executive; Chair of the National Cyber Study Group
August 29, 2008	Closed briefing. Judy Baker Senior Manager, Strategy, Communications and Policy Centre for the Protection of National Infrastructure

August 14, 2008	Closed briefing. Robert Lentz Deputy Assistant Secretary of Defense for Information and Identity Assurance
July 28, 2008	Closed briefing. David Wennergren Deputy Chief Information Officer, Networks and Information Integration, Department of Defense
July 25, 2008	Closed briefing. National Cyber Investigative Joint Task Force, FBI
June 12, 2008	Closed briefing. Office of the National Counterintelligence Executive
June 4, 2008	Public event: Cybersecurity and Critical Infrastructure Protection: Is There a Better Strategy? Keynote speaker: Roger Cumming Deputy Director, Centre for the Protection of National Infrastructure
May 27, 2008	Closed briefing. Defense Information Systems Agency and the Joint Task Force on Global Network Operations • General James E. Cartwright (USMC) Vice Chairman of the Joint Chiefs of Staff • Lieutenant General Charles E. Croom Jr. (USAF) Director, Defense Information Systems Agency; Commander, Joint Task Force—Global Network Operations • Major General William T. Lord (USAF) Commander, Air Force Cyberspace Command (Provisional), Barksdale Air Force Base • General Jon M. Davis (USMC) Deputy Commander, Joint Functional Component Command—Network Warfare • Rod Beckstrom Director, National Cyber Security Center, U.S. Department of Homeland Security
May 22, 2008	Closed meeting. Tabletop cybersecurity exercises with the Central Intelligence Agency
May 8, 2008	Closed briefing. Shawn Henry Assistant Director, Cyber Division, FBI

May 8, 2008	Closed briefing. Melissa Hathaway Senior Adviser to the Director of National Intelligence and Cyber Coordination Executive; Chair of the National Cyber Study Group
April 28, 2008	Public Event: Views from Beyond the Beltway: Cybersecurity Recommendations from Experts. Keynote speakers: • John Koskinen Former Assistant to the President and Chair of the President's Council on the Year 2000 Conversion • Pamela Fusco Executive Vice President of Security Solutions, Fishnet Security • Stephen L. Squires Independent Consultant Panel: • Julie Ferguson Vice President of Emerging Technology, Debix • Jay Foley Founder Identity Theft Resource Center • David Mortman Chief Information Security Officer-in-Residence, Echelon One • Lisa Sotto Partner, Hunton & Williams
March 12, 2008	Public event: Improving Cybersecurity: Recommendations from Private Sector Experts. • Rodney J. Petersen Government Relations Officer and Security Task Force Coordinator, EDUCAUSE • John J. Suess Vice President of Information Technology/Chief Information Officer, University of Maryland • Larry Clinton President, Internet Security Alliance • John Carlson Senior Vice President, BITS, The Financial Services Roundtable

	• Steve D. Crocker Chair, Security and Stability Advisory Committee, Internet Corporation for Assigned Names and Numbers • Michael Aisenberg Principal, Federal Systems Security, MITRE Corporation • Guy Copeland Vice President, Information Infrastructure Advisory Programs, Computer Sciences Corporation
February 13, 2008	Closed briefing. Stewart A. Baker Assistant Secretary for Policy, U.S. Department of Homeland Security

Appendix D
List of Acronyms

APEC	Asia-Pacific Economic Cooperation
CCSO	Center for Cybersecurity Operations
CIO	chief information officer
CNCI	Comprehensive National Cybersecurity Initiative
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
DOS	Department of State
EOP	Executive Office of the President
FACA	Federal Advisory Committee Act
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FDCC	Federal Desktop Core Configuration
FDIC	Federal Deposit Insurance Corporation
FERC	Federal Energy Regulatory Commission
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FTC	Federal Trade Commission
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	industrial control systems
ICT	information communications technology
IRTPA	Intelligence Reform and Terrorist Prevention Act
ISAC	Information Sharing and Analysis Centers
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
JIACTF	Joint Inter-Agency Cyber Task Force
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center [query on this in text]
NCTC	National Counter Terrorism Center
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NITRD	National Information Technology R&D Programs
NOC	National Office for Cyberspace
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSTAC	National Security and Telecommunications Advisory Committee
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
R&D	research and development
SCADA	supervisory control and data acquisition
SEC	Securities and Exchange Commission
TIC	trusted internet connections
UN	United Nations
US-CERT	United States Computer Emergency Readiness Team
USTR	Office of the United States Trade Representative
WMD	weapons of mass destruction
WTO	World Trade Organization
Y2K	Year 2000