A REPORT OF THE
CSIS COMMISSION ON
CYBERSECURITY FOR
THE 44TH PRESIDENCY

Cybersecurity Two Years Later

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

Project Director
James A. Lewis

January 2011

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A REPORT OF THE
CSIS COMMISSION ON
CYBERSECURITY FOR
THE 44TH PRESIDENCY

Cybersecurity Two Years Later

Commission Cochairs
Representative James R. Langevin
Representative Michael T. McCaul
Scott Charney
Lt. General harry Raduege,
USAF (ret.)

Project Director
James A. Lewis

January 2011

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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, DC. 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 author(s).

Cover photo credit: Bolts of speed in blue binary tunnel pipe. © iStockphoto.com/ Anterovium/Hannu Viitanen.

© 2011 by the Center for Strategic and International Studies. All rights reserved.

ISBN 978-0-89206-625-4

Center for Strategic and International Studies
1800 K Street, NW, Washington, DC 20006
Tel: (202) 887-0200
Fax: (202) 775-3199
Web: www.csis.org

Contents

Cybersecurity Two Years Later

CSIS Commission on Cybersecurity for the 44th Presidency

I. Introduction

When CSIS published *Securing Cyberspace for the 44th Presidency*[1] two years ago, cybersecurity was not a major issue for public policy. Along with the work of many others, our first report helped to change this. However, the new energy in the national dialogue on cybersecurity has not translated into progress. We thought then that securing cyberspace had become a critical challenge for national security, which our nation was not prepared to meet. In our view, we are still not prepared.

2010 should have been the year of cybersecurity. It began with a major penetration of Google and other Fortune 500 companies, saw the Department of Defense describe how its classified networks had been compromised, watched the Stuxnet worm cut through industrial control systems, and ended with annoying denial of service attacks over Wikileaks. These public incidents were accompanied by many other exploits against government agencies, companies, and consumers.[2] They show how the United States is reliant on, but cannot secure, the networks of digital devices that make up cyberspace. As a nation, we must do more to reduce risk, and we must do it soon.

When major new technologies have appeared in the past, it has taken the United States decades to adjust its rules, policies, and practices to make them safer to use. In the nineteenth century, steamboats regularly blew up, but Congress waited 40 years until a long series of horrific accidents led to safety regulations. Automobile safety rules took more than half a century to enact and initially faced strong opposition from carmakers, who claimed that safety regulations would stifle innovation. Air safety regulations only appeared 23 after the first fatal crash. If this timeline holds for the Internet, which entered into commercial adoption in 1995, we may be years away from a creating a sufficiently secure information technology (IT) infrastructure.

Unfortunately, we cannot afford to wait years. The United States needs to rethink cybersecurity to fit a complex global network where connectivity, speed, and capacity create new possibilities for both the economy and for security. The global network will compel changes in business, technology, and security in ways that are not yet clear but will create new risks and new

---

[1] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, D.C.: CSIS, December 2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[2] A list of significant cyber incidents can be found here: http://csis.org/files/publication/110103_Significant%20Cyber%20Incidents%20Since%202006_0.pdf.

opportunities for those countries able to seize them. Our 2008 report had 25 recommendations for change. As we start a new year and a new Congress, we want to review where progress has been made on these recommendations and where action is necessary.

II. The State of Nature in Cyberspace

Why is it so easy to exploit cyberspace? The Internet was not designed to be a global infrastructure on which hundreds of millions of people would depend. That these 1970s technologies have worked so well and have so easily scaled to support 2 billion users is an amazing triumph, but anyone with malicious intent can abuse these networks.

Our chief opponents in cyberspace are nations with advanced capabilities. They have well-organized and well-financed militaries and intelligence services, employ thousands of people, with multimillion-dollar budgets to overcome our cyber defenses. Expecting the private sector to defend against these professional opponents is like saying we can use our airlines to defend our national airspace against enemy fighter aircraft. We still have no defense against advanced cyber power.

However, we are not engaged in a cyber war. Short of armed conflict, nation-states are unlikely to launch cyber attacks against the United States. The political risk is too high. Just as with missiles and aircraft, countries can strike the United States using cyber attack, but they know this would trigger a violent if not devastating response. The risks are too high for frivolous engagement.

Nor are denial-of-service attacks, such as those used by the defenders of Wikileaks, an act of war. Perhaps a denial-of-service attack, if it was sufficiently massive and sustained for a long period of time, could be regarded as warfare, but large-scale denial-of-service attacks happen every day against government agencies, critical infrastructure, and companies. Most have learned to deal with them. They are akin to noisy and annoying protests, not war. Nor are there, as of yet, examples of terrorism from cyber attacks. While terrorists do not face the same constraints on use as nations-states, they have not used cyber attacks. Should this change, the United States is unprepared to defend itself.

The greatest threats remain espionage and cyber crime. Espionage and cyber crime are not acts of war. They are, however, routine occurrences on the Internet. The Internet provides nation-states, their intelligence agencies, and cyber criminals with vastly expanded capabilities to illicitly acquire information. Economic espionage does the most damage: other nations steal technology, research products, and intellectual property. Some cyber spies are nation-state agents, some are proxies acting for a nation-state, and some steal for their own benefit.

High-end cyber crime takes two forms. Criminals steal intellectual property (IP), either at the behest of a government or for their own use. Even small companies can be a target. Estimates of these losses are in the billions of dollars. Germany, whose economy is one-quarter the size of the U.S. economy, estimated its own IP losses due to industrial espionage at $25 billion to $50 billion, the bulk of which results from weak Internet security. Most companies do not report losses and may not even be aware of them. When Google was hacked, only one other company reported a potential loss, even though we know that more than 80 major companies were victims.

Advanced cyber criminals have capabilities that approach those of national intelligence agencies, and some criminals have close relationships with their governments. A flourishing black market supports cyber crime. In it, you can buy the latest malware, learn of recently discovered vulnerabilities, or rent "botnets" (thousands of computers remotely controlled for criminal purposes without the computer owners' knowledge). Credit card numbers, personal information, and bank account data can be bought in bulk. Some sellers offer guarantees.

Cyber criminals also target the financial system, going after automated teller machines (ATMs), online bank accounts, and credit cards. Some crimes have been spectacular: one Russian gang took $9.8 million from ATMs over a Labor Day weekend. The chief planner is not only still at large, we do not even know his or her identity. Where law enforcement is weak, cyber criminals are safe.

Our 2008 report concluded that cybersecurity is now one of the major national security problems facing the United States and that only a comprehensive national strategy consistent with U.S. values would improve the situation. Many in the current administration share these conclusions, but progress has been slow. Cybersecurity unavoidably takes second place to more immediate concerns, such as the wars or the economy. This is understandable, but the result has been that despite good intentions, many important actions have been deferred.

III. The Policy Context

Cybersecurity is intrinsically complex, involving national security, commercial interests, and privacy concerns. The United States remains unsure about how to proceed. Our policies have not kept up with technology or the emergence of the global network. Discussion remains wedded to ideas developed when the Internet was smaller, largely American, and much less important for our economic life. These policies are no longer adequate for global commerce and national security, but there is real resistance to change.

Presidential Decision Directive 63 of 1998, the 2003 *National Strategy to Secure Cyberspace*, and the 2008 Comprehensive National Cybersecurity Initiative, put a voluntary, disaggregated approach based on information sharing and public-private partnership at the center of cybersecurity policy. This approach faces a number of intractable problems. First, it assumes incorrectly that private entities will share adequate amounts of information, despite liability, antitrust, and business competition risks. Second, it underestimates the difficulty of sharing classified information with the private sector. Finally, it assumed that if all parties had adequate information about threats, they would take action. Despite these problems, a voluntary, disaggregated approach based on information sharing and public-private partnership remains the center of cybersecurity policy.

The United States needs to rethink its policies and institutions for cybersecurity to fit a global network where connectivity, speed, and capacity create new possibilities for both the economy and security. The implications of this shift for business, technology, and security are not yet clear, but they will be significant. The process of rethinking cybersecurity will be difficult, but this situation is not new. *Securing Cyberspace for the 44th Presidency* called for a new approach. We recommended a coherent national strategy, a new organization to lead the effort, and a federal

decision to make cybersecurity a national priority by stepping in where the market had been unsuccessful.

Our recommendations for cybersecurity were well received and are reflected in the May 2009 *Cyberspace Policy Review*.[3] However, while our recommendations were well received, their implementation has been mixed. This is largely a reflection of the toll taken by the many crises the administration has faced, but it also reflects internal disputes over the importance of cybersecurity and the role of the federal government in advancing it.

For example, on May 29, 2009, the president declared cyberspace as a critical national asset that the United States would use all means to defend. This was a crucial first step for securing cyberspace, but it is only a first step. The president also announced the creation of a cybersecurity coordinator in the White House—something we recommended (albeit at a more senior level)—but it then took the administration seven months to fill this position.

Several factors explain the slow progress. The most significant was the idea that the Internet must be open, untrammeled, and remain the Wild West if there is to be innovation. The creators of the Internet believed cyberspace would become a self-organizing global community led by private action, where governments should play only a limited role. It would become, in this rosy view, a global commons where people could invent and create without constraint. The problem is that the lack of constraints empowers malicious activity as much or more as innovation. Other governments increasingly reject this pioneering American vision as inadequate for securing what has become a critical global infrastructure.

When we wrote our report in 2008, we did not expect that Internet advocates would so strongly oppose cybersecurity because it ran counter to this pioneering ideology. Some Internet companies actively lobbied against stronger measures during the drafting of the administration's *Cyberspace Policy Review*. It is ironic that one such company was a victim of the Google hack, reflecting in part a belief that, as one White House official put it, "the Internet community would solve the cybersecurity problem without the need for government," and that an Internet Wild West was preferable, as it would accelerate innovation.

It is facile to assume the gains from innovation enabled by an unrestricted Internet outweigh the losses from economic espionage. It does little to help innovation and growth if foreign competitors can steal by the truckload the results of U.S. investments in research and intellectual property because of weak cybersecurity.

Unsurprisingly, protecting "turf" played a role. Cyber functions are scattered across the executive branch. Reorganization could mean that some offices would have to surrender control. The different offices argue that this would put important equities that they now oversee at risk. Turf concerns intertwine with the conceptual dispute over innovation, economics, and the nature of the Internet. The cabinet agencies also have little interest in supporting a stronger White House role in cybersecurity, as it would diminish their independence.

---

[3] The White House, *Cyberspace Policy Review* (Washington, D.C.: The White House, May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

This quest to protect innovation generated strong opposition to the idea of cybersecurity regulation. It may come as a surprise to some that the administration opposed regulating the private sector, but this opposition grew out of a blend of Internet ideology and the feckless 2003 *National Strategy to Secure Cyberspace*,[4] which called for a voluntary approach to cybersecurity.

There is vocal hostility in the United States to regulation, for reasons both good and bad. Overregulation or prescriptive regulations will damage growth. Deregulation and market forces usually produce better economic outcomes, but there are issues—consumer safety or national defense—where the market response will always be inadequate. Few Americans would abolish the Federal Aviation Administration and assume that airlines would of their own volition consistently do what is needed to ensure safety of flight.

Americans usually assume that market processes will solve problems without government intervention. It is not surprising that there are obstacles and objections to altering our approach to cybersecurity. These technologies have become fundamental to our way of life and any significant change to how they operate should face serious scrutiny and assessment. The process of rethinking cybersecurity will be difficult, but this situation is not new. Every time a new technology has emerged to reshape business, warfare, and society, there has been a lag in developing the rules needed for public safety. Cyberspace is different only in its global scope and in its urgency.

IV. Ten Key Areas for Progress

Two years after our first report, we have taken a step back to ask where the United States stands in this difficult but essential national effort. We have identified 10 key areas where the nation must take action. We provide a brief overview of developments and suggest tangible and necessary outcomes that provide metrics to gauge progress in the next two years.

1. **Coherent organization and leadership for federal efforts for cybersecurity and recognition of cybersecurity as a national priority.**

While the administration's *Cyberspace Policy Review* provided the framework for a comprehensive approach, the United States still lacks an integrated national cybersecurity strategy. An integrated approach creates synergy, signals other countries that U.S. indifference is over, and can help avoid an uneven response. We understand a strategy is being developed. In the interim, action has moved to individual agencies. Initiatives at the Departments of Defense (DOD), Homeland Security (DHS), State, and the Federal Bureau of Investigation (FBI) have made cybersecurity a high priority.

The United States divides primary responsibility for cybersecurity between DOD and DHS. DHS is developing a national response plan, has an effort to better secure civilian agency networks

[4] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

using the various Einstein technologies,[5] and is increasing its cyber workforce. DHS opened the National Cybersecurity and Communications Integration Center (NCCIC), a DHS-led watch and warning center. NCCIC combined the U.S. Computer Emergency Readiness Team, the National Coordinating Center for Telecommunications, and integrated the National Cybersecurity Center (NCSC), which coordinates operations among the six largest federal cybersecurity centers.

The October 2010 Memorandum of Agreement between DHS and DOD[6] was a significant development for federal efforts. It clarifies how the National Security Agency (NSA) will support DHS in its cybersecurity efforts, allowing NSA's technical and intelligence capabilities to be used for homeland defense. Under the DOD-DHS Memorandum of Agreement, NCCIC is assisted by a Cryptologic Support Group from NSA that provides access to specialized intelligence and technical skills.

Perhaps the most noteworthy changes in federal cybersecurity are at DOD, where the civilian and military leadership have led the federal government in making cybersecurity a priority, developing strategies, and allocating resources. The most significant development is the creation of the new U.S. Cyber Command that will centralize many of DOD's existing cyber functions for both defense and offense and provide powerful new capabilities.

Our first report called for this kind of consolidation in the Executive Office of the President, with a new National Office of Cyberspace. Led by an assistant to the president, the office would work with the National Security Council to manage the many aspects of cybersecurity, while protecting privacy and civil liberties. Although the administration created a cybersecurity coordinator and a new office, we still believe that the nation will ultimately need something like the Office of the U.S. Trade Representative to lead and coordinate federal policy for what has become a central element of national security and economic life.

In the White House, the Office of Management and Budget (OMB) has been a source of progress. It is making significant revisions to the implementation process for the Federal Information Security Management Act (FISMA) to create a dynamic and automated assessment of agencies' security. It is developing focused standards for "cloud" security. These initiatives will make the federal government more efficient, and they substantially reinforce cybersecurity in the "dot gov" environment.

The goal for 2011 should be to issue a comprehensive national strategy based on new ideas rather than recycling the 2003 strategy. This means no appeals to public-private partnerships, information sharing, or unilateral efforts at deterrence, as were made in the 2003 strategy. National strategies tend to be anodyne expressions of general goals. An effective strategy would set specific objectives drawn from our first report and the 2009 *Cyberspace Policy Review* and assign timelines and responsibilities for achieving them.

---

[5] Programs to monitor networks for malicious activity and perhaps (for the most advanced technologies, known as Einstein III) interdict the malicious payload before it reaches its targets. Einstein is currently deployed only on government networks.

[6] Department of Homeland Security, "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," October 13, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

2. Clear authority to mandate better cybersecurity in critical infrastructure and develop new ways to work with the private sector.

The current situation is as follows: DHS—working with the National Institute of Standards and Technology (NIST) and OMB—defends all "dot gov" space; and DOD defends all of the "dot mil" space for military and intelligence networks. But no one in particular defends private networks, where our policy is to rely on some combination of individual action, encouragement, leadership by example, and faith in market forces. We faced this same situation in 2008.

Adam Smith, the eighteenth-century Scottish economist who is considered the father of capitalism, would tell us that national security and public safety always require more than the market can deliver. The September 2010 Stuxnet incident, where a highly advanced piece of malicious software (malware) penetrated and damaged Iranian nuclear facilities, is a harbinger of what is to come. The market will not deliver adequate security in a reasonable period, and voluntary efforts will be inadequate against advanced nation-state opponents.

Our recommendation in our first report was that we need a new, cooperative approach to regulation in four essential infrastructure sectors.[7] And we still believe this is best. Regulation needs to impose the lightest possible burden, be flexible rather than prescriptive, and be developed in partnership with industry. Precedents for these flexible regulations can be found in recent developments such as the changes to the implementation of the Federal Information Systems Management Act reporting guidelines or the consensus audit guidelines developed by a consortium of federal agencies and private organizations.[8]

One approach would be to have DHS and the "first-party regulators" (e.g., the existing regulatory agencies) work together to extend existing regulation to cover cybersecurity. Some sort of reimbursement or incentive structure to cover any additional costs could accompany an extension of existing regulation.

Most existing public-private partnerships would need to change significantly to provide this advice. The federal landscape remains crowded with public-private partnerships, committees, and advisory bodies with some involvement in cybersecurity. One reason that many existing public-private partnerships in cybersecurity have contributed so little is that there is no regulatory backbone to give companies and agencies "skin in the game." A better model for effective partnerships can be found in DOD's Defense Industrial Base effort and the Enduring Security Framework, which are successful because of high-level participation by all parties and the existence of binding contractual relationships.

---

[7] Electrical power and energy, telecommunications and information technology, financial services, and government services.

[8] OMB, "Memorandum for Heads of Executive Departments and Agencies: FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," April 21, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf; John Gilligan, "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (Version 2.1)," August 10, 2009, http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf.

Draft legislation that drew on the precedent of how DHS regulates the chemical sector using risk-based performance standards[9] offered the possibility of real improvement in cybersecurity. Measures attached to the Defense Authorization Act also would have improved cybersecurity, and we are disappointed that Congress was unable to act on these bills. This bipartisan legislation would have done much to remedy this problem. The administration and Congress should make it a priority to enact effective legislation this year.

Identifying progress in 2011 will be simple. If the nation passes laws and the administration issues effective regulations for critical infrastructure, there has been progress. These should include mandatory improvements in authentication of identity for critical infrastructure. No regulations mean inadequate progress.

3. A foreign policy that uses all tools of U.S. power to create norms, new approaches to governance, and consequences for malicious actions in cyberspace. The new policy should lay out a vision for the future of the global Internet.

In 2008, we recommended that the United States develop a strategy to engage other nations, including our opponents, on cybersecurity and that this international effort use all tools of U.S. power—diplomatic, military, and economic. We discussed how nonproliferation provided useful precedents. Other precedents for cybersecurity governance include the Financial Action Task Force, a multilateral body that sets rules to counter money laundering, and the International Civil Aviation Organization, a global body the United States and its allies created at the dawn of international air travel to ensure that flight between countries was safe.

International engagement has become even more important in the last two years as nations seek to extend sovereign control into cyberspace. Cyberspace is not a commons; other countries have realized this and are acting to protect their own sovereign interests. Existing governance bodies created by the United States now face challenges from those who wish to end American "hegemony" over the Internet.

The struggles over the Domain Name System (DNS) and the Internet Corporation for Assigned Names and Numbers (ICANN)—and the problems at the International Telephony Union (ITU), a UN body that coordinated telecommunications activities—all reflect efforts to exert greater control of the Internet. Other nations with very different political values are challenging the original, U.S.-centric idea of governance by a private, global community. The United States needs to articulate a positive agenda of norms, consequences, and cooperation. The agenda needs a vision of how the international community will manage cyberspace to ensure continued openness, connectivity, and security. Secretary of State Hillary Clinton's January 2010 speech concerning the Internet was a vital first step, but the United States does not have a strategy for engaging others at a time when powerful nations are moving to reshape the Internet to better serve their interests.

The previous administration preferred a unilateral policy and confined multilateral discussions to a sterile exchange of best practices. The Obama administration has made engagement a central

[9] Chemical Facility Anti-Terrorism Standards, a regulatory process administered by DHS. For more information, see http://www.dhs.gov/files/laws/gc_1166796969417.shtm.

element of its cyber efforts and announced some months ago that it would develop an international strategy. After years of blocking any discussion in the United Nations of cybersecurity, the United States helped in 2010 to develop an initial framework for international cooperation. The United States won NATO support to make cybersecurity a priority at the recent Lisbon summit and is developing collective cyber-defense arrangements with NATO and other allies. Similar bilateral discussions should also be encouraged.

These are encouraging steps, but the slow pace of norms building and the lack of effective trade measures are disquieting. There are still few consequences for malicious activity in cyberspace, and there are no cooperative structures to create such consequences. The theft of intellectual property violates World Trade Organization (WTO) commitments, and some would argue that restrictions on the free flow of information are also violations. Yet, while the *2010 Joint Strategic Plan on Intellectual Property Enforcement*[10] mentions how the Internet has created new risks, it focuses entirely on piracy of entertainment products and does not mention the multibillion dollar losses of intellectual property that occurs through cyber espionage—a startling omission. This is the sort of disconnect that could be avoided by a comprehensive strategy and strong coordinating office.

The State Department announced the creation of a senior cyber coordinator position but has not explained how the new position will coordinate with the many jostling bureaus in the department that already claim some control of cybersecurity. One approach to resolving this would be to have the new coordinator perform a role based on the precedent of the State Department's counterterrorism office, where a coordinator forges partnerships with other governments and provides coherence to U.S. international strategies.

Real progress requires engagement with other countries. This means that the United States must put forward proposals to other governments for norms and other confidence-building measures. Operationalizing some sort of collective defense among allies would be a sign of improvement. Another measure of progress would be an increase in the number of indictments, convictions, and extraditions from the countries that are havens for cyber crime. Direct engagement bilaterally or in the WTO on the failure to protect IP in cyberspace is another. Working groups or internal discussion papers are not enough. Progress in winning international agreement on norms, collective defense, cyber-crime prosecutions, and IP protection will let us gauge international efforts for cybersecurity.

4. An expanded ability to use intelligence and military capabilities for defense against advanced foreign threats.

In reaction to a foreign penetration of a classified network in December 2008, DOD made cybersecurity a departmental priority. The cornerstone of this approach is the creation of U.S. Cyber Command, a new joint command that unifies DOD's offensive and defensive cyber activities. Cyber Command is just part of a larger effort to engage allies, develop strategy and

[10] Executive Office of the President, *2010 Joint Strategic Plan on Intellectual Property Enforcement* (Washington, D.C.: Executive Office of the President, June 2010), http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf.

doctrine, and train personnel. The military services support Cyber Command with strong efforts to train cybersecurity specialists. The creation of Cyber Command is a major step forward for the United States. However, use of military capabilities will require resolving a number of doctrinal and policy issues, including when a military response is appropriate and how cyber actions would be authorized.

DOD, working with DHS, has begun an approach currently named "Active Defense" that can be described as working with tier 1 service providers to intercept malware from foreign sources. How far into the domestic infrastructure this Active Defense should extend and how a nervous privacy community can be reassured about the intent of such programs remain major issues.

Even if existing legal authorities allow for an expanded DOD role in defending critical infrastructure, the "perception problem" remains significant.

Any discussion of an expanded military role in defending civilian networks runs into powerful antibodies that grow out of civil liberty and privacy concerns. Historical precedent also limits the role of the military in civilian affairs. New "network neutrality" principles issued by the Federal Communications Commission may further complicate any policy decisions. We do not advocate changing the traditional separation that exists between military and civilian functions but believe that the administration and Congress should clarify our policies and laws to allow the military to fulfill its traditional role in protecting against foreign threats. Finding a way to do this in partnership with DHS and the private sector remains a fundamental challenge for cybersecurity policy. Making better use of military and intelligence capabilities against advanced foreign opponents, in partnership with DHS and the private sector, remains a fundamental challenge for cybersecurity policy.

The clearest metric for progress is a decision on how to use DOD capabilities to protect domestic targets. The DOD-DHS Memorandum of Agreement is a good first step, but the United States must determine how it will use DOD capabilities in the "dot com" domain. The most visible metric would be an executive order or some other presidential document to guide military and intelligence activities in protecting critical infrastructure. Since any decision will require working with those outside the government, a highly classified, unreleasable document, like the 2008 Comprehensive National Cyber Initiative (CNCI), will be inadequate.

5. Strengthened oversight for privacy and civil liberties, with clear rules and processes adapted to digital technologies.

Safeguarding privacy and civil liberties is of paramount importance for the United States. There is a persistent belief that cybersecurity must inevitably damage privacy. The source of this concern is that government will collect and use information in inappropriate ways, for political purposes, law enforcement, or administrative actions. The previous administration's decision to initiate a massive communications surveillance campaign in the wake of the September 11, 2001, terrorist attacks reinforced these concerns. Whether this campaign was necessary is a subject of debate, but it was done in secret and without judicial or congressional oversight. The effect, in combination with weak consumer privacy protection in the United States, has been to create powerful antibodies to cybersecurity initiatives that appear to infringe on privacy or civil liberties.

As we move to active defense and cloud computing, the requirements for oversight and the protection of privacy and civil liberties will increase. The increased importance of oversight comes at a time of decreased capability and public confidence in those entities tasked with such oversight. The toll of the debate over renewal of the Foreign Intelligence Surveillance Act, warrantless surveillance, and other new security initiatives taken since 2002 has been to erode existing oversight arrangements and, as a result, public acceptance of important security efforts.

The CSIS Commission's 2008 report emphasized the central importance of protecting privacy and civil liberties as part of a comprehensive cybersecurity program. This was also a key element of the *Cyberspace Policy Review*, which recommended that a privacy and civil liberties official be a core member of the proposed (NSC) cybersecurity directorate. The chief weaknesses, we would judge, are the unnecessarily adversarial relationship between security and privacy and the continuing weakness of oversight mechanisms.

The White House recently announced that the Privacy and Civil Liberties Oversight Board (PCLOB) would be reestablished, after a two-year hiatus. The White House has also set up another interagency group to look at privacy issues, and the administration has announced the creation of a National Program Office to lead consumer privacy policy activities in the Commerce Department. These are useful steps, but privacy policy for cybersecurity remains a confusing melange of individual agency products and borrowings from intelligence oversight policies (such as Executive Order 12333). The administration needs to work off a sound and transparent set of principles to ensure that privacy and civil liberties are protected and to strengthen institutions like the PCLOB so that those principles become real.

The key metric for success is frequent and regular activity demonstrated by public reports and a higher degree of transparency in cybersecurity actions. DHS's Privacy Impact Assessment for Einstein technologies is a useful precedent.[11] A PCLOB that is transparent in its processes and regularly provides public reports on its work will begin to rebuild the trust needed for better cybersecurity.

6. Improve authentication of identity for critical infrastructure.

We wrote in 2008 that an anonymous Internet can never be secure, but that is what we still have. Efforts to require some level of authentication face immense resistance from a vocal minority. Our recommendation was limited to requiring critical infrastructure to meet a higher standard. This would affect fewer companies and no consumers. While this would be only a partial solution to making the Internet a less malevolent place, our view remains that mandatory standards for authentication of identity in critical infrastructures is a fundamental requirement for homeland and national security.

The new "National Strategy for Trusted Identities in Cyberspace"[12] (NSTIC) takes a tentative step toward fixing this problem, but it does not go far enough for critical applications. Early drafts of

[11] DHS, "Privacy Impact Assessment for the Initiative Three Exercise," March 18, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf.
[12] The White House, "National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy," draft, June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.

the NSTIC were a pastiche of previous policies reflecting sharp internal divisions over the role of the private sector and the need for regulation. The biggest challenge for the NSTIC and its new National Program Office in the Department of Commerce will be to increase incentives for people to use online authentication. An appeal to adopt stronger authentication because of the unrealized potential benefits for e-commerce is not enough. Technologies for better authentication of online identity have been around for more than a decade, but many people and companies have chosen not to use them. The new National Program Office should quickly fund pilot projects that prove the technical feasibility of an identity system and the value of having Internet credentials based on in-person proofing.

We still believe an interim step that mandates the use of stronger authentication by critical infrastructure companies is both feasible and the best solution. Survey data show that the situation has not changed very much since 2008. Some companies do a good job; others (about half) still rely on easily cracked passwords to secure sensitive functions, including control systems. Our recommendation for critical infrastructure is to move beyond the NSTIC and take a pragmatic approach based on in-person proofing, better standards for credential issuance, and the elimination of password-only access to critical infrastructures.

Issuance of a stronger NSTIC is one metric for success in 2011. Active pilot projects by the National Program Office would be another. The best measure of progress would be the issuance of a more focused set of requirements for critical infrastructure.

7. Build an expanded workforce with adequate cybersecurity skills.

Our November 2010 report, *A Human Capital Crisis in Cybersecurity*,[13] focused on cybersecurity workforce improvements. It noted the shortfall in trained personnel for cybersecurity and called for expanded education and rigorous certification. There are many initiatives underway, and our report proposed that the nation build on this existing work to remedy the shortfall. The cybersecurity community can now identify practices that reduce risk. These practices can be taught and their results (in terms of reducing successful penetrations or the exfiltration of data) can be measured. There was considerable debate in our commission as to the maturity of computer science in general and cybersecurity in particular as a discipline to which we can apply rigorous, objective standards of skill and practice. There was agreement, however, that rapid action is needed to increase the number and skill level of those who practice in this area. However, as with much else in cybersecurity policy, the problem has been identified, initial steps have been taken, but there has been slow progress in changing the situation from where we were two years ago.

Numbers provide the metric for progress: Is the United States graduating from its schools more people with the skills necessary for improving cybersecurity, including the skills needed for incorporating cybersecurity into the industrial control systems used in critical infrastructure?

[13] Karen Evans and Franklin Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* (Washington, D.C.: CSIS, November 2010), http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf.

8. Change federal acquisition policy to drive the market toward more secure products and services.

The federal government can use its purchasing power to incentivize the development of more secure products and services. Requirements to deploy Domain Name System Security Extensions (DNSSEC)[14] in top-level "dot gov" domains are examples, building on earlier successes of initiatives like the Federal Desktop Core Configuration. Government purchases of new security solutions will both drive down the cost of those solutions and serve as a proving ground for their effectiveness. The government is in a better position than the private sector to be an early adopter of new technologies.

The more challenging task involves deciding how to use acquisitions to create a more trustworthy supply chain. Heavy-handed measures, such as intrusive product inspections by national agencies, will backfire by reinforcing the plans of other nations to use these techniques. Some combination of transparency into the provenance of products and assurance that they meet international standards will be essential, but it also will be crucial to pursue a multilateral approach, perhaps building on Common Criteria[15] or expanding current efforts like those of the industry-DOD Open Group, to increase trust across the supply chain process.

The metric for success is straightforward: federal acquisitions require government agencies to buy more secure products or services.

9. A revised policy and legal framework to guide government cybersecurity actions.

Congress wrote most of the laws governing cybersecurity activities in the 1970s and 1980s, for different purposes and earlier technologies. We are still using these laws, but they can create unintentional obstacles to information sharing and cooperation. Other laws that need reexamination include the Telecommunications Act of 1996, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, the Communications Assistance to Law Enforcement Act, and Sections 2510-2522 and Sections 3121-3127 of 18 U.S.C. (known as Title III and the Pen/Trap Statue, respectively). Some service providers also believe that antitrust laws prohibit them from sharing information on cybersecurity threats between competing businesses.

Legislation introduced in 2010 began the process of examining how to modernize existing legislation, and several committees continue to review existing legislation. This is a good start for a long overdue task, but absent any forcing event, we expect a long debate over the appropriate legal framework for cybersecurity. Many of us fear, however, that we will see no action on cybersecurity absent some overwhelming crisis, which will produce unnecessarily draconian legislation.

Federal policies governing cybersecurity activities are also out of date. Agencies now comply with department-level guidance that implements the Privacy Act of 1974 or that is derived from Executive Order 12333, which was written to govern intelligence collection activities. The result is unintended restrictions that hamper interagency cooperation without increasing privacy. A case

[14] DNSSEC is a protocol to secure the Domain Name System, part of the Internet's addressing service.
[15] Common Criteria is an international standard for certifying the security of computer technologies.

in point is malicious code that contains the phrase "Bugger Microsoft." Under current rules, agencies would treat this as data referring to a U.S. person, greatly constricting the ability to share it outside of the collecting agency and limiting access to malicious signatures or other data essential for cyber defense. An executive order specifically written to govern cybersecurity would improve both government performance and civil liberties safeguards.

Measurable goals for progress include the introduction and passage of constructive legislation to modernize existing laws and the drafting and signing of presidential directives for agencies clarifying and formalizing the powers and responsibilities of agencies for their cybersecurity activities.

10. Research and development (R&D) focused on the hard problems of cybersecurity and a process to identify these problems and allocate funding in a coordinated manner.

The new administration at the Defense Advanced Research Projects Agency (DARPA) has made cybersecurity research a priority. DARPA has initiated projects—named CRASH (Clean-slate Design of Resilient, Adaptive, Secure Hosts) and PROCEED (Programming Computation on Encrypted Data)—to develop more secure computing technologies.

Fundamental weaknesses in the Internet's mechanisms and networking protocols increase risk. The most significant problems are in the naming, numbering, and routing protocols, but there are many others. Both the hardware and software used in digital networks can be insecure, and software-based vulnerabilities are the technical path for criminals to capture personal computers. Hardware can be compromised in the factory or later in the supply chain. The physical and logical underpinnings of cyberspace are so complex that it will take years of sustained R&D to replace vulnerable technologies.

Important progress, however, is occurring outside of government or university channels. We are in another technological transition, moving to automated services and "cloud" computing, where we will depend on networks for essential services. Cloud computing has weaknesses, but it also offers the opportunity to aggregate and automate cyber defense. Much of the burden of security will shift from consumers and businesses to service providers that may be better equipped to meet advanced challenges. The move to the cloud is not a silver bullet that will solve all cybersecurity problems, but it is part of a larger move to a more mature infrastructure that includes the automation of security practices and monitoring—such as the Security Content Automation Protocol (SCAP)—particularly if we find a better way for service providers to work more effectively with government agencies.

R&D can often take years to produce results, so the best measurement of progress in the next two years will be sustained funding and attention to modernizing Internet technologies.

V. Prospects for Cybersecurity–2012

Most of the recommendations listed above appeared in our first report. Our review of the last two years found that there has been progress in almost all of the areas we identify as critical, but in no area has this progress been sufficient.

The findings of our first report still stand: cybersecurity is now a major national security problem for the United States; decisions and actions must respect privacy and civil liberties; private initiative alone will not produce security; and adopting a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure.

The cybersecurity debate is stuck. Many of the solutions still advocated for cybersecurity are well past their sell-by date. Public-private partnerships, information sharing, and self-regulation, are remedies we have tried for more than a decade without success. We need new concepts and new strategies if we are to reduce the risks in cyberspace to the United States.

Many are frustrated with pace of progress in cybersecurity. Analysts and senior officials in Washington talk privately about a "9/11" cyber-related scenario, reflecting a belief that as a nation, we will be unable to take any meaningful action on cybersecurity until after some large and damaging event. This need not be the case. We are united by a shared objective to protect our nation. This administration, working with the Congress (where both the Senate and the House have made cybersecurity a priority), can create a comprehensive national approach. If we can shed some of our old ideas, we can move decisively to secure cyberspace.

Where does this leave the nation as we start a new year? There are two possible outcomes in cybersecurity for the United States. We can continue to pursue outdated strategies and spend our time describing the problem until there is some crisis. Then it is likely that the United States will act, in haste, possibly with unfortunate consequences. Alternatively, we can take action on measurably effective policies. Our opponents still have the advantage, but we can change this.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1800 K Street, NW | Washington, DC 20006
Tel: (202) 887-0200 | Fax: (202) 775-3199
E-mail: books@csis.org | Web: wcsis.org

ISBN 978-0-89206-625-4