NATIONAL DEFENSE RESEARCH INSTITUTE

CHILDREN AND FAMILIES

EDUCATION AND THE ARTS

ENERGY AND ENVIRONMENT

HEALTH AND HEALTH CARE

INFRASTRUCTURE AND TRANSPORTATION

INTERNATIONAL AFFAIRS

LAW AND BUSINESS

NATIONAL SECURITY

POPULATION AND AGING

PUBLIC SAFETY

SCIENCE AND TECHNOLOGY

TERRORISM AND HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: Jump to Page 1

Support RAND

Browse Reports & Bookstore

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND National Defense Research Institute

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

A Cyberworm that Knows no Boundaries

Isaac R. Porche III, Jerry M. Sollinger,
Shawn McKay

Prepared for the Office of the Secretary of Defense

Approved for public release; distribution unlimited

NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted within the RAND National Defense Research Institute, a federally funded research and development center sponsored by OSD, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2011 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

The report that a sophisticated cyberworm called Stuxnet had been planted on the computers of an Iranian nuclear facility and had damaged processing equipment sent a tremor across many governments and industries. Although many computing technology experts had known that such an attack was theoretically possible and that less-capable versions had been demonstrated, Stuxnet served notice on the world that a threshold had been crossed. The event raised numerous questions about the ability of the U.S. government and commercial firms to defend their networks against assaults by worms, viruses, and other malware.

This paper explores some of the issues raised by sophisticated yet virulent malware, including the nature of these threats, the vulnerabilities they exploit, and the characteristics that make defending against them so difficult, especially the knotty problems posed by organizational and legal restrictions. It also provides a brief assessment of where U.S. defensive capabilities stand and what needs to be done to improve them. Although this paper considers cyberspace from a U.S. military perspective—that is, as a so-called "warfighting domain"—the considerations presented here translate easily to a broader view of cyberspace as a global commons.

This research was conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community. For more information on the Acquisition and Technology Policy Center, see http://www.rand.org/nsrd/ndri/centers/atp.html or contact the director (contact information is provided on the web page).

Questions and comments about this research are welcome and may be directed to the lead author, Isaac Porche (porche@rand.org).

Contents

Preface iii
Figures and Tables vii
Summary ix
Acknowledgments xiii
Abbreviations xv

A Cyberworm That Knows No Boundaries 1
The Difficulty of Defending Cyberspace 2
How to Identify an Attack 5
What Was Needed to Carry Out the Attack 6
The Implications of Stuxnet and Similar Worms 7
Implications of the Success of Stuxnet 8
What Is Needed to Defend Against Stuxnet and Similar Worms 9
How Organizational Boundaries Hinder Efforts to Mount an Effective Defense 10
  Intragovernmental Limitations 10
  Intersectional Limitations 11
Conclusions 12
  The Threat of and Opportunity for Real Damage from Cyberspace Is Increasing 12
  Not All Attacks Can Be Prevented 13
  The Best Defense Includes an Offense 13
  Current Organizational Boundaries Hinder Identification and Mitigation 14
Recommendations 15
Future Work 16

APPENDIXES
A. The Cyberspace Domain 19
B. Worms 21
C. Einstein Intrusion Detection and Protection 25
D. Federal Cyber Legislation 27

Bibliography 33

Figures and Tables

Figures

A.1. Cyberspace Today 19
A.2. Cyberspace and Social Networking 20
B.1. Conficker Worm Progression 23

Tables

1. Selected Relevant U.S. Organizational Initiatives, Laws, and Reviews 11
2. Organizational Strengths and Weaknesses of Federal Agencies in Defending U.S. Cyberspace Infrastructure 14
3. Examples of Proposed Legislation Regarding the Assignment of Federal Roles in Cyberspace 16
D.1. Federal Cyber Legislation 28

Summary

Iran's announcement that a computer worm called Stuxnet had infected computers that controlled one of its nuclear processing facilities marked a signal event in cyber attacks. Although such attacks were known to be theoretically possible, the Stuxnet incident proved that a cyberworm could indeed be planted in a system and produce physical damage. Furthermore, the sophisticated nature of the worm and the resources that would have been required to design, produce, and implant it strongly suggest a state-sponsored attack.

Although the implications of the attack are still unfolding, three are immediately discernable. First, it ends the debate about whether such worms are feasible. Clearly, they are. Second, Stuxnet-like worms pose a serious threat. The creators were able to implant the worm on computers that were almost certainly not connected to the Internet, and they were apparently able to mask its presence even while it was modifying the signals that the industrial control systems were sending. Reportedly, the worm damaged hundreds of gas centrifuges. Industrial control systems are ubiquitous; they control electrical power, gas, refineries, and many other systems. The ability to tamper with them and cause physical damage is worrisome. Third, the fact that Stuxnet apparently required the resources of a nation (and perhaps more than one) suggests a new willingness on the part of governments to use cyber attacks to further national goals.

Purpose

This paper explores the implications of Stuxnet-like worms for the United States and specifically for the U.S. Department of Defense. It discusses what makes cyber defense difficult and outlines the bureaucratic and legal issues and boundaries in the United States that can compound the problem. It then offers some conclusions and recommendations for how the United States can confront the increasing risk posed by such threats.[1]

Why Cyber Defense Is Difficult

Stuxnet aside, fending off cyber attacks is difficult. The inherent characteristics of cyberspace favor the attacker, not the defender. Furthermore, unlike conventional or nuclear war, a cyber attack is not always obvious. Additionally, the responsibility for defending the nation against a cyber attack spreads across many federal agencies and the private sector, which complicates

[1] Stuxnet revealed vulnerabilities that could prove inviting to adversaries planning future attacks (see Harris, 2008, p. 62).

mustering a coherent response to an attack. Legal boundaries govern who can do what in response to such attacks, so it will be necessary to sort through these issues to ensure that when an attack comes—and we believe one surely will—government agencies can work in concert with private-sector organizations either to blunt the attack's effects or to minimize the damage afterward.

Cyberspace Favors the Attacker

Several characteristics of cyberspace tilt the playing field in favor of the attacker. First, cyberspace has no boundaries, which means that an attack can come from virtually anywhere. It takes only a computer and an Internet connection to obtain a passport to cyberspace. Individuals with sinister intentions can mask their electronic identity or steal one from an unsuspecting individual, either by collecting the information required to take on the purloined identity or by using a "bot" to take over a computer that can be used to enable or perpetrate the attack. Second, cyberspace changes constantly. Sites are added and dropped daily, which means that assuming a new identity is far easier in cyberspace than it is in the physical world.

What this means is that it is not possible to stop all attacks. Firewalls and intrusion prevention systems will thwart only so many attacks.[2] Defenders must be right all the time; the attacker, only once.[3] Careless use of a portable hard drive, the failure to update virus protection software, a compromised password, and dozens of other events can open the door to an attack.[4] Thus, a key policy focus must be how to respond once an attack has occurred.

Cyber Attacks Are Hard to Identify

Mounting a response to a cyber attack requires knowing that one has occurred, and in cyberspace that is not necessarily easy. Malicious activity is common in cyberspace, but not all such activity constitutes an attack. Some examples are phishing expeditions designed to steal personal or financial information, efforts to obtain proprietary information from private-sector firms, and or simple hacking attempts to penetrate computer systems for the purpose of espionage. These are not technically classified as attacks but, rather, as espionage attempts.[5] However, they could pave the way for more destructive activity, or they could be used to plant a worm that, at some later time, could launch its own attack. Presumably, this is the way Stuxnet was programmed to operate. Worms can lie dormant until the circumstances they have been

---

[2] In his guide to the Certified Information Systems Security Professional exam, Shon Harris states that an intrusion prevention system is intended "to detect [nefarious] activity and not allow the traffic to gain access to the target [e.g., the network or device] in the first place" (Harris, 2008, p. 260). An intrusion prevention system is supposed to be an advancement over intrusion detection systems, which are configured to "spot something suspicious happening on the network" (Harris, 2008, p. 250).

[3] This is, of course, also the case with terrorism.

[4] According to the U.S. Army Information Assurance Training Center (undated),

> Malware is an acronym that stands for MALicious software and it comes in many forms. Generally speaking, malware is software code or snippets of code that is designed with malice in mind and usually performs undesirable actions on a host system.

[5] Such collection activities or probes are known as computer network exploitation and are differentiated from computer network attacks, which seek to destroy, alter, or degrade capabilities.

built to exploit appear,[6] and only then do they become active. Thus, the actual "attack" can occur days, weeks, or even months after the initial exploit.

Bureaucratic and Legal Issues Can Hamper Defense

Defending against worms like Stuxnet requires excellent capabilities marshaled into a coherent and coordinated response. The United States has plenty of the former but, in our view, has difficulty with the latter. Responsibilities can overlap or conflict. For example, stealing financial information is a crime, and the Federal Bureau of Investigation is charged to deal with such criminal activity. But the U.S. Department of Homeland Security has a mandate to protect the civilian agencies of the federal executive branch and to lead the protection of critical cyberspace. The former would include the federal banking system, and the latter could include the nation's banking system. Good intelligence has always been a prerequisite to good defense, but many attacks come from overseas locations. Therefore, efforts to garner intelligence outside the United States would involve the agencies authorized to do so. Many regard the National Security Agency as the most capable government entity when it comes to analyzing and defending against cyber attacks (see Clarke and Knake, 2010, p. 37; Dilanian, 2011; Alexander, 2010a, 2010b; and Shanker and Sanger, 2009). But legal limits constrain what the U.S. Department of Defense can do. Much illicit activity masks itself in emails, but privacy laws preclude the extent to which the government can monitor such transmissions.

None of this is to say that these limitations cannot be overcome. Indeed, a number of proposed pieces of legislation attempt to deal with them. Furthermore, federal agencies have improved their ability to effect the kind of coordination needed to deal with these problems. However, the challenge is great and is compounded by the speed needed to respond to increasingly sophisticated threats. Worms can be scrubbed from systems if its administrators know the systems have been breached. But they need to act quickly, or the worm will have done its damage and then erased itself.

Conclusions and Recommendations

This examination of Stuxnet and similar threats and their implications resulted in the following observations and conclusions:

- The threat of and opportunity for real damage from cyberspace is increasing.
- It is not possible to prevent all attackers from intruding on all networks and devices.
- The best defense includes an offense.
- Current organizational boundaries hinder efforts to successfully identify and mitigate intrusions.

Accordingly, we recommend additional congressional action to grant new authorizations that accomplish at least the following two goals:

[6] There is also a school of thought that such exploits constitute cyber crime if they can be identified as misuse under the Council of Europe Budapest Convention on Cybercrime (Robinson, 2011). The tenets in the Budapest Convention are cited in the President's *International Strategy for Cyberspace* (2011).

- Enable substantially better collaboration among the various government organizations that have a role in cyberspace and between these organizations and the private sector.
- Grant *at least one capable organization* the authority to track cyber intruders and criminals with the same freedom of maneuver that these adversaries enjoy. New authorities must be established for this to occur and it will likely require substantial revisions to the U.S. Code—undoubtedly a daunting challenge—and significant public debate.

These recommendations will require additional analysis and further development. However, as goals, they are essential to informing that process.

There is no simple solution to the threat posed by adversaries in cyberspace. Clearly, one challenge is determining how best to navigate within the requirements and expectations of a democratic society that relies heavily on its computer systems and networks, against an enemy that has no boundaries and can act with impunity in the face of national or international norms and legal frameworks.

Acknowledgments

This paper benefited greatly from comments from several of our RAND colleagues. Edward Balkovich provided insightful comments on an early draft. RAND Army research fellow LTC Michael York and Chad Serena also shared their expertise. Our two peer reviewers, Mark Sparkman and Neil Robinson, gave us the benefit of their knowledge of the topic and helped us clarify many aspects of the paper. We are grateful to all of them.

Abbreviations

DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
ICS	industrial control system
ICS-CERT	Industrial Control System Computer Emergency Readiness Team
IP	Internet protocol
IT	information technology
NSA	National Security Agency
P2P	peer to peer
SCADA	supervisory control and data acquisition

A Cyberworm That Knows No Boundaries

In 2009, cyber security analysts worldwide reported that a "worm" called Stuxnet had penetrated and, in all likelihood, damaged an Iranian nuclear facility.[1] The attack was apparently prosecuted through the facility's industrial control system. Iran later confirmed that Stuxnet had indeed infected computers and control systems in its uranium enrichment complex at Natanz and had damaged centrifuges there.[2]

The nature of the incident did not surprise those who had known that such an attack was theoretically possible (see, e.g., Edwards and Stauffer, 2008). The likelihood of such a targeted attack was revealed as long ago as 1997, when a U.S. Department of Defense (DoD) exercise known as "Eligible Receiver" demonstrated the ability to gain surreptitious access to computers that controlled an electric power grid plant.[3] A decade later, the U.S. Department of Energy's Idaho National Laboratory showed that it could insert malicious code into a closed network to inflict severe physical damage on an industrial generator. Indeed, Stuxnet may not have even been the most successful or catastrophic cyber attack on a supervisory control and data acquisition (SCADA) system. Thomas Reed, in his 2004 book *At the Abyss: An Insider's History of the Cold War*, describes how, in 1982, a Trojan horse was inserted into Canadian software designed to control natural gas pipelines; this software was then "allowed" to be stolen and used by the Soviets. According to Reed (2004, p. 269), "[T]he pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space."

While Stuxnet may not have been the first of its kind, it did cross significant thresholds in terms of capability and, more importantly, employment. The capability it demonstrated is impressive. Its creators very likely penetrated air-gapped, closed networks, which enabled Stuxnet to worm its way into a nuclear control system. However, of more significance is the fact that Stuxnet now represents the most well-known instance of a state-sponsored cyber attack against another government that reportedly resulted in physical damage. This attack may change accepted norms of cyberspace behavior. Its success has alarmed other industries

---

[1] A *worm* is an unwanted software program secretly planted on a computer that enables (among other things) someone other than the owner to control it. The name "Stuxnet" is an anagram of letters found in parts of its code.

[2] Iranian President Mahmoud Ahmadinejad was quoted admitting that Stuxnet was "successful in making problems for a limited number of centrifuges with software installed in electronic devices" (see, e.g., Winter, 2010).

[3] Owens, Dam, and Lin (2009) describe the exercise as one that was "designed to expose weaknesses in computer security in unclassified DoD computer systems using off-the-shelf technology and software downloaded from hacker websites," adding that it "demonstrated how hackers might disrupt troop deployments."

and other countries about what it might portend. Specifically, any country's infrastructure controllers (e.g., control systems for electric power, gas, water, refineries, and many other types of infrastructure) could fall victim to such a targeted worm.[4] Mounting a defense against these threats will require a level of coordination among agencies of the government and the private sector that has rarely—if ever—been achieved.

This paper uses the Stuxnet attack as a starting point to explore the issues related to defending a nation's industrial systems against malware and similar intrusions. First, we describe the inherent characteristics of cyberspace that make establishing a defense so difficult. We then turn to an analysis of the operation of Stuxnet, the damage it caused, and how the worm must have behaved to wreak the damage it did. We also take up the issues of establishing an effective cyber defense in the United States against malware like Stuxnet and the challenges of doing so within the rules dictated by the current laws, regulations, and policies that are likely to constrain the most robust efforts to coordinate a defense. This topic holds interest for multiple audiences: policymakers, legislators, cyber operators, government officials, and staff of commercial firms that are involved with or concerned about cyber security.

The Difficulty of Defending Cyberspace

The critical distinguishing characteristic of cyberspace is that it has become a "global commons," existing almost everywhere, open to anyone, allowing its inhabitants to move across it with ease and at ever-increasing speeds.[5] From a defensive perspective, it is difficult to imagine how to defend a space that has no boundaries, changes constantly, lets anyone in, and exists virtually everywhere. Even so-called closed networks, such as those that are not connected to the Internet (i.e., air-gapped networks) are still at risk from the manual insertion of malware (by means of portable storage devices); even wireless code insertion, transmitted over radio or radar frequencies, is conceivable (Clarke and Knake, 2010, p. 7; Fulghum, 2011).

People often talk of "defending U.S. cyberspace" in much the same way that they speak of defending the country's borders. The difficulty is that cyberspace really has no boundaries. The data, services, and applications in cyberspace flow across routers and servers that span the globe.

Thus, the so-called U.S. cyberspace cannot be fenced off.[6] Some portions are within territorial borders, but others are not. For example, server farms in Canada support the near-ubiquitous BlackBerrys carried by government officials and private-sector employees. Real-world barriers have no counterparts in cyberspace. Nor do electronic barriers offer sanctuary. While organizations can (and should) build electronic "firewalls," such defenses can be breached or bypassed.

---

[4] These systems often use what are known as programmable logic controllers.

[5] We use the metaphor *cyberspace* to refer to the worldwide network of information infrastructure (e.g., routers, servers, connections among them), telecommunications networks, and computers, including the applications (e.g., social media programs) facilitated by the infrastructure. Like all metaphors, it has its limitations, but it is useful here because it highlights a misconception that can hinder effective responses to threats and vulnerabilities: that there is a physical space that can be defended. A more illustrative description of cyberspace is provided in Appendix A.

[6] We acknowledge that this paper takes a U.S.-centric view of cyberspace and that other nations may not hold the same view.

The components of cyberspace are constantly being created, destroyed, moved, lost, physically relocated, hidden and exposed, and connected and disconnected. The kaleidoscopic change of cyberspace occurs at the speed of light (or at least at the speed of a keystroke). This is due partly to the pace of the evolution of information technology (IT) in general, which, in turn, drives the pace of the evolution of cyberspace. New products appear daily, and these products can receive updates weekly. For these and other reasons, threats and vulnerabilities in cyberspace differ from those in the world of conventional combat.[7] Because they can develop and appear almost overnight, countering them is especially difficult. The same is true from the attacker's perspective. Networked systems are continually changing and evolving, making it potentially difficult to exploit a vulnerability.

Cyberspace lets anyone in, even some who may not want to be there (or who do not even realize they are there). A trip into cyberspace does not require a passport or a background check. It is open to anyone who has an electronic device that can link to the Internet: those who want to do good and those who intend to do ill; those who want to provide information and those who would steal it; those who want to spend money and those who want to make it; those who want access to factual information and those who want to corrupt that information. All enjoy equal access. Ubiquitous access makes establishing a defense especially difficult. Is the packet of information asking for entry to a server what it says it is, or is it a disguised piece of malware that intends to offload data from the site and sell it? Not only does cyberspace grant anyone access, it lets anyone be whomever he or she wants to be. As the famous *New Yorker* cartoon by Peter Steiner pointed out, on the Internet, no one knows you are a dog. No one knows whether you are a criminal, either.

Cyberspace can incorporate the unwilling, too. Neither "wire" nor consent is required for one to be represented in cyberspace.[8] Air gaps are difficult to maintain and thus no longer sufficiently protect devices from nefarious actors who operate in cyberspace.[9] The Natanz computers were, in all likelihood, not intended to be connected to the Internet (or any other network), but that did not stop someone from placing malware on them. As long as a device is not dumb (that is, as long as it contains a processor and some memory), it can be accessed, affected, and controlled to some degree by anyone who can overcome the air gap.[10] For example, a person could access or tamper with the device and insert code (intentionally or unwittingly). This is the so-called "sneakernet" that overcomes air gaps. The proliferation of wireless, handheld devices that connect to the Internet has opened millions of additional paths to cyberspace.

---

[7] A threat is a "potential danger to information or systems" (Harris, 2008, p. 61). A vulnerability, according to Harris (2008, p. 61), is "a software, hardware, or procedural weakness that may provide an attacker an open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment."

[8] Wireless devices with memory and processors, such as laptops, printers, and gaming devices, are as common as similar devices that network with an actual Ethernet cable (i.e., a "wire").

[9] An IT device does not have to be connected to the Internet to be affected by actors operating in cyberspace; an air gap cannot protect a device from a worm infestation, for example. Another way to think of an air gap (between an IT device—with memory and processors—and cyberspace) is as a long period of latency with intermittent connectivity. The point is that cyberspace users can undermine both types of air gaps.

[10] Although the network targeted by Stuxnet was likely closed (i.e., not connected to the Internet), it was still "sucked into cyberspace" because the computers that accessed it also accessed open networks. These computers were (reportedly) laptops used by technicians who plugged into the facility's programmable logic controllers, which are on the closed network, to maintain and diagnose equipment. These same laptops could also be used by the technician to access email, which would connect them to an open network.

Electric power is also not a requirement to participate. Modern corporate badge readers and electronic tollbooths communicate with inert badges or cards. Many devices and appliances, such as printers and cell phones, have wireless connections and can be surreptitiously turned on and accessed (McCullagh, 2006; "Canadian Researchers Uncover China-Based Electronic Spying Operation," 2009). Thus, unplugging a device from the Internet does not protect it from being remotely affected (and becoming a part of cyberspace).

Cyberspace is the polar opposite of bounded physical space: It is everywhere. With wireless devices, people can access cyberspace from virtually anywhere on Earth, and they can go anywhere within cyberspace that is not protected by sophisticated firewalls; if they are relatively skilled, they can get behind firewalls as well.

Threats and vulnerabilities can originate anywhere, including the usual suspects (e.g., known hackers) or even well-intentioned amateur code writers.[11] A malicious hacker with a laptop and a seat in an Internet café has everything needed to launch an attack in cyberspace. Alternatively, a well-intentioned but naïve "app writer" can accidentally propagate a useful utility that unlocks backdoor access.

Defending against an attack from the Internet, which is composed of many Internet-protocol (IP)–based networks, is inherently difficult for many of the reasons already discussed. Compounding this difficulty is the problem of identifying the source (i.e., the author) of an attack, due, in part, to the relative anonymity afforded by IP networks. This is not to say that it is impossible, especially given enough time and resources to fuse multiple sources of intelligence. A 2011 White House initiative to encourage the voluntary use of Internet IDs, the National Strategy for Trusted Identities in Cyberspace, was motivated largely by this difficulty. If the initiative is successful, it may alleviate some of the difficulty even if only slightly. The intent is to create a trusted regime in which the U.S. public and private sectors can operate, treating the nonparticipants as "outside the perimeter of trust" (Balkovich, 2011).

The upshot of the inherent nature of cyberspace is that no country or private-sector organization can prevent attacks entirely.[12] Intruders will eventually succeed in penetrating the computers and controllers that organizations depend on. Cyber defenders are at a distinct disadvantage: It takes only one person, one device, one opportunity to compromise one component of a system.[13] New systems often mean new vulnerabilities. Intruders will always find vulnerabilities to exploit and thus can almost always gain access to a system in one way or another. And once in, they can be difficult to detect and dislodge.[14]

---

[11] This group could include software developers, mobile application developers, developers of widgets used to enhance open-source browsers, and so on.

[12] Appendix B includes a more detailed discussion of the specific capabilities of Stuxnet and other recent breaches by worms.

[13] This is a viewpoint espoused by DoD. According to Deputy Secretary of Defense William Lynn (2010b),

> In cyberspace, the offense has the upper hand. . . . [T]he U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. . . . In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls.

[14] The rapid pace of app development for mobile devices may accelerate the birth rate of software vulnerabilities. Likewise, techniques to exploit these vulnerabilities evolve just as rapidly. For example, the Conficker worm morphed on a monthly basis. See Appendix B for a more detailed discussion of Conficker and other worm attacks.

In fact, an argument exists that the best way to defend is to take offensive action in a form termed *active defense*.[15] For example, Owens, Dam, and Lin (2009, p. 16) state that active defense includes both the "neutralization of an attacker's ability to attack and the imposition of costs on the attacker for the attack." The authority to proceed in this manner (attack and counterattack) is a potential bottleneck that can limit the ability to operate at the "speed of cyber." In mid-2011, the Associated Press reported that President Obama signed orders to clarify authority and permission with regard to when presidential approval (a slow process) must be obtained (Baldor, 2011). According to the article, exploit (or intelligence) missions are preapproved, but not those actions that deploy viruses and worms.

Cyber fights go on constantly. Increasingly, they are fought inside networks as a series of "block-to-block" engagements (between system administrators and interlopers) that is more akin to running street battles in Somalia in 1999 than trench warfare of World War I.

There are many parallels to draw from in thinking about the nature of conflict in cyberspace. Police protection is one. Consider conventional crime, such as robbery or burglary. It has never been eliminated, and it occurs regularly in every community, despite locks, alarms, gates, laws, and penalties. As a result, every community has a police force to identify the activity and arrest the criminals so that they can be removed (at least temporarily) from civil society. Police patrols or officers responding to calls exist to give chase and apprehend criminals.[16]

Protecting cyberspace requires a similar approach. The aggravating factor in attempting such patrols in cyberspace is that cyber boundaries are virtually nonexistent, and "giving chase" requires transiting international borders and public and private networks. One implication of the uniqueness of cyberspace is that no single organization in the United States has the permission or unilateral authority to execute the type of patrol and chase needed to protect its interests.

How to Identify an Attack

By the accounts cited, Stuxnet *evolved* into what has been accepted as a cyber attack. However, a generally accepted definition of a cyber attack does not exist. This is a challenge to defense in cyberspace. For example, many network penetrations are made to garner sensitive or otherwise protected information—in other words, to spy. But does pilfering such information constitute an attack? Historically, spying has not been seen as a reason to go to war. However, it has been suggested (Robinson, 2011) that a reading of the Council of Europe's Budapest Convention on Cybercrime yields an interpretation that simply having been hacked justifies a response.

---

[15] Concisely, the term means "to eliminate or degrade an adversary's ability to successfully prosecute an attack" (Owens, Dam, and Lin, 2009, p. 13). One part of the approach is to acquire good intelligence on threats and vulnerabilities (through covert or other means). At the most general level, a good defensive tactic is to try to anticipate the nature and origin of an attack before it occurs. Software developers try to write code with specific threats in mind. However, this is no trivial task even for an industry titan like Microsoft.

[16] The U.S. Department of Homeland Security (DHS) employs a more elaborate analogy than our "cops-and-robbers" metaphor: It equates defensive strategies in cyberspace with the human body's immune system (Ananthaswamy, 2009; DHS, 2011). One strategy resulting from the analogy is that defensive efforts involve cooperation among devices in cyberspace. Specifically, defensive efforts at the local (cellular) level in one system work within a global system (like blood circulating throughout the body).

Responding to an attack can also be difficult because it is not always clear when one has occurred or who did it. The insertion of Stuxnet provides a case in point. The effects reportedly manifested sometime after the worm was implanted. Allegedly, it remained dormant until the specific set of circumstances that its programming called for had occurred. Even then, the evidence indicates that the attack was not instantaneous. Rather, the worm executed its programming in gradual steps. In theory, at least, a worm could remain dormant for months or longer before it acted.

The challenge for the defender is to know whether the attack mechanisms have been initially implanted, ideally before the attacker accomplishes whatever end is being sought. This would require the defender to notice subtle anomalies in the system that would signal that a firewall had been breached or that a piece of malicious code had been implanted.

What Was Needed to Carry Out the Attack

Stuxnet provides a good case study of the types of capabilities a defense must be prepared to counter. Analysis of available information suggests the worm was *not* the work of a single ingenious hacker (Fulgham, 2011). As noted in a 2011 Symantec report (Falliere, Murchu, and Chien, 2011), Stuxnet's great complexity would require significant resources to develop.[17]

Speculation about what was needed to develop and carry out the attack includes the following:

- The developers were able to gain access to the industrial controller's schematics and design documents. (For example, was the facility using Siemens controllers? Which versions? Which operating systems, patches, upgrades?)
- They would have needed to obtain the associated Siemens industrial controllers, as well as technical and design documentation.
- Perhaps they also acquired centrifuges similar to those in the Iranian facility.
- They obtained knowledge of the computing environment in the facility.
- It is likely that they set up a mirrored environment that would include the necessary industrial controllers and other hardware, such as the programmable logic controllers, to test the worm.
- They would have needed to obtain at least two compromised digital certificates.
- They needed knowledge of unknown or unpublished (i.e., zero-day) exploits in Microsoft software.
- Finally, they developed a means to implant the worm on computers or portable flash drives that might eventually be connected to the programmable logic controllers (Falliere, Murchu, and Chien, 2011; Broad, Markoff, and Sanger, 2011).

All of the above, we maintain, imply a case of espionage. For example, covert operations conducted by intelligence agencies are one likely means to infect computers, through either a

[17] According to the report, Stuxnet was the first malicious code to "exploit four 0-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator" (Falliere, Murchu, and Chien, 2011, p. 55). See Appendix B for a discussion of zero-day exploits.

physical breach or social engineering,[18] especially those that are not routinely connected to the Internet (Owens, Dam, and Lin, 2009, p. ix). Also implied is the need for substantial financial resources (to acquire industrial controllers and set up a test facility), as well as access to personnel to provide the broad technical expertise required.[19] Open-source estimates suggest that dozens of people with a range of skills (e.g., programmers, software engineers) took many months to develop Stuxnet (see, e.g., Gross, 2011, who puts the number at 30).

The Implications of Stuxnet and Similar Worms

As discussed thus far, Stuxnet was a significant and, in its own way, impressive achievement that exposed the extent of threats and vulnerabilities alike. What can be done once can usually be done again, which means that worms like Stuxnet can also threaten important U.S. industries and infrastructure.

Stuxnet is, reportedly, a piece of self-replicating malware that inserts itself into the Siemens software that is used to operate industrial control systems (ICSs) (Broad, Markoff, and Sanger, 2011).[20] It seems to work by reprogramming the instructions issued by the ICS. In the case of the Iranian nuclear facility, the worm's target appears to have been the gas centrifuges that are critical to the uranium enrichment process. According to reports, over a period of months, the worm subtly changed the motor-control frequencies that drive the centrifuges, thus affecting their spin rate and accelerating them to the point where they became unstable and failed.[21] According to a report by the Institute for Science and International Security, between November 2009 and January 2010, Iran replaced 1,000 IR-1 centrifuges at its Natanz fuel enrichment plant (Albright, Brannan, and Walrond, 2010).[22]

The *New York Times* reported on speculation that Iran's nuclear developmental efforts had been "set back by several years" and that Stuxnet was a primary contributor (Broad, Markoff, and Sanger, 2011). The extent of the damage continues to be debated and remains unclear.[23]

Even more worrisome is the apparent stealth that was built into Stuxnet: It appears to have been programmed to hide its activities by sending false information to the displays that

---

[18] Social engineering is not a technique limited to cyberspace. However, for the purposes of this discussion, it is a term that refers to gaining access to a computer or network by tricking (fallible) humans—for example, asking people (for example, on the phone or via email) for their passwords by pretending to be their company's IT department. Kevin Mitnick wrote about this in his 2002 book, *The Art of Deception: Controlling the Human Element of Security*. Social engineering can be practiced by cyber criminals and state actors alike.

[19] Including but not limited to knowledge of centrifuge design limitations, motor-control devices, programmable logic controller software, and relevant operating systems.

[20] Edwards and Stauffer (2008) define an ICS as a broad set of control systems, including SCADA, distributed control, process control, energy management, automation, and safety instrumented systems.

[21] See Chien, 2010, for a recent Symantec report on Stuxnet.

[22] The report cites data from the International Atomic Energy Agency indicating that an unusual number of centrifuges were not operating during this period. The authors caveat the assessment by noting that the IR-1 centrifuge is known to have a high failure rate, although the report maintains that Stuxnet probably contributed to a portion of the 1,000 replacements.

[23] If the extent of the damage turns out to be limited, there is an argument about the cost-benefit ratio of the Stuxnet effort. For the purposes of our assessment, Stuxnet is an example of potential damage, irrespective of the actual damage caused by this incident.

monitored system performance.[24] The operation was elegant in many regards, and this is but one example. By some accounts, it continues to change and plague the Iranian government's operations (Broad, Markoff, and Sanger, 2011).

Implications of the Success of Stuxnet

The implantation of Stuxnet and the successful execution of its instructions are worrisome for at least four reasons. First, the incident ends the debate about whether such a worm is even possible. It is real, and it can do serious physical damage. Second, the sophisticated nature of the worm and the substantial resources required to produce it make it all but certain that it was a state-sponsored effort. This means that the event was not the result of some whiz-kid hacker, or even a more sophisticated criminal enterprise to which a state turned a blind eye. The effort required sophisticated knowledge of the Siemens software and other components that ran the ICS, something not easy and certainly not cheap to obtain. Stuxnet also required significant manpower in terms of programmers and software engineers. Since it is very likely that the Natanz facility was not connected to the Internet, it also implies that some sort of clandestine effort was involved in getting the worm into the system. True, such insertions can be accomplished by relatively simple methods (e.g., leaving a flash drive in a parking lot with the hope that a curious or well-meaning individual will plug it into a computer that is connected to the ICS to determine what is on the drive), but even that tactic would mean that someone had the wherewithal to get the drive into Iran and plant it near a secure facility.

A third implication is that control systems other than those for nuclear power plants could be co-opted. The list of control systems that, if penetrated, could wreak substantial damage is long: electrical grids, systems that facilitate financial transactions, air and rail transportation systems, water and sewage systems, and even systems in space, such as the Global Positioning System (GPS). While it is unclear exactly how vulnerable these systems are, the experience of Stuxnet suggests that the most prudent course is to treat them as though they are vulnerable and to determine what steps should be taken to protect them.

This leads to a fourth cause for concern: All of these systems involve both private and government entities. Trying to coordinate defensive activities across government agencies is challenging enough. Add the private sector into the mix, and coordination efforts become even more complex and thus more difficult.

The ability of a worm like Stuxnet to affect the systems on which so many depend makes defense everyone's problem; if GPS were to go down, the outage would affect not only those who are trying to navigate their way to a meeting in a strange town or a ship charting its course to port but also military units that depend on GPS for location information and weapon systems that depend on it for accurate delivery. A disrupted power grid would affect government and civilian organizations alike.

Some experts downplay such threats and vulnerabilities (see Libicki, 2009). They point out, accurately enough, that the first thing that happens after a breach is that programmers

[24] According to the *New York Times* article, Stuxnet also "secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart" (Broad, Markoff, and Sanger, 2011).

and system engineers go to work to plug the gap. In that sense, cyber attacks are self-defeating, since their very attack calls into being the means to overcome them. While true enough, we would argue that this position does not take fully into account an attack using a worm like Stuxnet. Public reports suggest that such a worm, once implanted in a system, can lie dormant for long periods until it senses the precise combination of circumstances it is designed to exploit. When they do occur, it carries out its programming, and the damage is done: The centrifuges are destroyed, the electrical grid has collapsed, or the financial transactions have been disrupted. In short, it has done its work, and plugging the gap will not rectify the damage (though it may preclude repetition of this particular worm).

What Is Needed to Defend Against Stuxnet and Similar Worms

As we contend in this paper, state sponsorship makes it difficult to defend against Stuxnet-like worms. A state can devote substantial manpower to cyber warfare, but defending against a state-level threat will require the best capabilities available in industry and government. Fortunately, the United States has some very good capabilities in both sectors. However, it will take a coordinated effort and therein, we maintain, lies the challenge or—more accurately—one of the challenges.

Law, bureaucracy, and tradition all combine to affect the cooperation and coordination that must occur to mount an effective defense. Laws govern what classified information can be shared between the government and the private sector.[25] The organizational rules and boundaries that define the specific functions of government agencies can have a similar effect. A cyber attack launched, say, against a financial system can legitimately be considered a crime and fall within the purview of law enforcement agencies. But, by law, DHS is charged with certain cyber responsibilities; its functions in cyberspace are to "protect the federal executive branch civilian agencies (the "dot-gov"), and to lead the protection of critical cyberspace" (Lute and McConnell, 2011). A major financial network arguably could be seen to be a part of critical cyberspace.[26] And effective defense requires good intelligence. For attacks launched from overseas, good intelligence would require the services of agencies authorized to collect information in those locations—the Central Intelligence Agency and the National Security Agency (NSA). Attribution remains a difficult but necessary task.

A complicating factor is that passive defense alone may not necessarily suffice. Retaliation (if in the national interest) requires determining who did what after an attack and precluding the next assault. Recent announcements that the United States may respond kinetically or conventionally to a cyber attack focus on this need (Spillius, 2011; *International Strategy for Cyberspace*, 2011). But we contend that a more desirable goal would be to know what is likely coming next, because a very rapid response might be required, particularly against what are known

[25] Robinson (2011) notes that a disparity can exist between what the legislation says "on the books" and what occurs in practice. Other studies (e.g., European Network and Information Security Agency, 2009) address this point tangentially.

[26] This is not to say that the government has not taken steps to mitigate the problems associated with organizational limitations. The FBI, through its participation in the National Cyber Investigative Joint Task Force, coordinates its efforts with other government agencies. See FBI, undated.

as "zero-day" attacks. Zero-day attacks exploit software vulnerabilities that are unknown to developers.[27] These types of attacks require responses within hours or days.

Testimony abounds that the most capable U.S. government agency with respect to cyber intelligence and security is the NSA (Shanker and Sanger, 2009; Clarke and Knake, 2010). It has the people, resources, and access to information required to build a defense. As stated earlier, other agencies have roles as well, so in our view, the challenge becomes one of harnessing the many capabilities at hand into one coherent response. Doing so across government, law enforcement, and private organizations presents many hurdles, especially from the complex legal environment (e.g., Title 10 versus Title 50 in the U.S. Code, the federal criminal code in Title 18). Appendix C explains how DHS relies on the NSA to help develop and implement one of the DHS's more vital network monitoring programs, called Einstein.

How Organizational Boundaries Hinder Efforts to Mount an Effective Defense

The biggest hurdle that must be overcome in efforts to defend against Stuxnet-like worms is not technical, as formidable as that challenge might be. We contend that the organizational rules that a defense must cope with to be effective are even more problematic. The many government agencies that are called upon to help protect cyberspace are bounded by laws, regulations, and policies that govern what they can and cannot do, a selection of which are listed in Table 1. These limitations fall into three categories: intragovernmental, intersectional, and privacy protection.

Intragovernmental Limitations

As mentioned earlier, different government agencies have different cyber responsibilities. This makes perfect sense in many ways because different agencies have different capabilities, so they should be tasked to do what they are good at. The trick is to harness all the capabilities to a common end, and therein lies the problem. Cyber defense requires a coherent response, and the bureaucratic responsibilities as currently articulated hinder progress toward that goal.

In our view, the initiatives listed in Table 1 have not resolved the intragovernmental coordination issues. Indeed, one of the major criticisms made in the President's 60-day cyberspace policy review concerned the current patchwork nature of policies caused by the evolution of IT and the diverse government agencies specifying policy and publishing regulations. The review recommended creating a cybersecurity coordinator position on the National Security Council (later signed into law by President Obama).[28] One of the main functions of the cybersecurity coordinator is to fuse the current patchwork of cyber policy into a cohesive continuum (*Cyberspace Policy Review*, 2009). If successful, it might eliminate some of the uncertainty regarding the current cyber boundaries, as long as these policies are shared.

---

[27] *Zero day* is the term for the day the attack is discovered, not the day it is launched, thus suggesting that the intended damage may have already occurred. See Appendix B for a more detailed discussion of this concept.

[28] According to the Executive Office of the President, "The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative." President Obama determined that the initiative and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These activities will play a key role in supporting the achievement of many of the key recommendations of 60-day review.

Table 1
Selected Relevant U.S. Organizational Initiatives, Laws, and Reviews

Initiative	Date	Purpose and Boundary Implications
Presidential Decision Directive 63, Policy on Critical Infrastructure Protection	May 22, 1998	Created the formal relationship between the U.S. government and the private sector concerning the protection of critical infrastructure, including in cyberspace; specifically, establishes the role of Information Sharing and Analysis Centers (see National Council of ISACs, undated)
Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection	December 17, 2003	Established DHS as the focal point for cybersecurity coordination across government and private sector; updated Presidential Decision Directive 63
U.S. Code, Title 47, governing communications	As of February 1, 2010	Requires Internet access providers to be capable of supplying the government with real-time forensics of Internet traffic
National Security Presidential Directive 54/Homeland Security Presidential Directive 23, Cyber Security and Monitoring	January 8, 2008	Established the Comprehensive National Cybersecurity Initiative and identified key roles and responsibilities across the federal government
President Obama's 60-day cyberspace policy review	May 2009	Offered many recommendations for new cyber strategies, response plans, and cyber coordinators; as of October 2010, two recommendations were fully implemented and 22 were partially implemented
ICS Computer Emergency Response Team (ICS-CERT) creation	2009	Established a public-private forum for information sharing and response to ICS cyber threats and vulnerabilities
Creation of a cybersecurity coordinator position on the National Security Council	December 2009	Provided greater transparency of federal cyber activities through central coordination by the White House
Memorandum of agreement between DHS and DoD regarding cybersecurity	October 13, 2010	Described DoD collaboration with DHS on cyber activities; DoD assigns a senior NSA official to work closely with DHS

Intersectional Limitations

Intersectional limitations refer to those between the public and private sectors. Presidential Decision Directive 63 recognized that any attacks on critical U.S. infrastructure would likely include facilities in both the public and private sectors. For each of 15 major economic sectors (e.g., transportation, financial), the designated lead agency would appoint a liaison officer to work with the sector on cyber defense. While a helpful step, we argue that such appointments did not necessarily deal with all the necessary issues.

The government and the private sector alike have stressed a continued need to enhance transparent information sharing, including the sharing of sensitive information from both sides, but the private sector has voiced concerns about this boundary. These concerns include protection of proprietary information, trade restraints due to intrasector collaboration, reputation harm, and liability or regulatory consequences due to sharing information (*Cyberspace Policy Review*, 2009; Business Software Alliance et al., 2011). In some cases, this is the very information needed to mount an effective defense. However, the concern is both natural and warranted.

On the other side of the coin, it is important for the government to disseminate timely and relevant cybersecurity information to operators of critical infrastructure in the private sector. Communication of potential Stuxnet-like attacks against the private sector is a goal of ICS-CERT, an organization in DHS. A critical issue here is that many U.S. companies that use these potentially vulnerable control systems are actually international companies, with offices located in foreign countries and, in many cases, largely staffed by foreign nationals. Releasing sensitive cybersecurity information to such companies opens up the possibility of compromise.

The relationship, mandated or voluntary, between government and the private sector is another intersectional issue that must be addressed. There are notable examples, such as the FBI's Infragard partnership and ICS-CERT.[29]

Government regulations will come in the form of standards the private sector must follow.[30] Both the government and the private sector have advocated standardization as a main tenet to enhance cybersecurity (DHS, 2011), but standardization has its consequences. The complex, static, and checklist nature of the current electric power system standards have reduced the ability of private-sector utilities to respond dynamically to today's cyber threats and vulnerabilities to the electrical grid (Assante, 2009). Cyber issues associated with public-private partnerships encompass the balance between mandated and voluntary engagement, the proper empowerment of the private sector to protect its own assets, and the protection of sensitive information that flows between the private sector and the government.

To mount a successful national defense in cyberspace, these and other issues need to be fully understood, vetted, and aligned. The degrees of freedom in such a process are limited and must respect civil liberties.

Conclusions

The Threat of and Opportunity for Real Damage from Cyberspace Is Increasing

Cyberspace is a domain and a global commons whose reach is being constantly expanded by wired, wireless, and sneaker-netted connectors. Everything from home thermostats to the critical infrastructure that is vital to daily life (water, power, manufacturing) is within its reach. It is "shared by all" and dominated by none.

Stuxnet demonstrated how the ever-expanding cyber realm can also be thought of as an active battlespace in which nation-states can be attacked and, to paraphrase Clausewitz,

---

[29] InfraGuard is a partnership between the FBI and the private sector. According to the partnership's website, the organization is dedicated to sharing information to prevent hostile acts—including cyber attacks—against the United States (Infraguard, undated). It is a "Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003." In an ironic twist, it has been reported that the organization itself was hacked and that passwords and other information may have been stolen (Dockery, 2011).

Besides informing key private-sector partners, ICS-CERT will respond to Stuxnet-like attacks on SCADA systems in both the government and the private sector. Private-sector interaction with ICS-CERT is voluntary. A particular company that has suffered a cyber attack on its ICS may request help from ICS-CERT but is not obligated to invite ICS-CERT within its facility (McGurk, 2011).

[30] One current proposal suggests a mandatory cybersecurity checklist for private firms, with penalties for breaches (Nakashima, 2011).

advance policy by other means.[31] It also exposes how a country's infrastructure can be threatened by a determined, well-funded adversary with good knowledge of existing vulnerabilities.

Not All Attacks Can Be Prevented

Cyber intrusions are constant and nearly impossible to stop completely, especially in light of the susceptibility of the IT supply chain, which spans many countries, friend and foe.[32] Deputy Secretary of Defense Lynn (2010b) has said of the state of DoD networks, because "intrusions will inevitably evade detection and not be caught at the boundary, U.S. cyber defenses must be able to find intruders once they are inside. This requires being able to hunt within the military's own network." A continuous effort to mitigate intrusions into networks and other nodes in cyberspace is necessary.[33] This effort is about identifying the sources of these compromises and removing them.

The Best Defense Includes an Offense

The Office of the Secretary of Defense advocates a "dynamic defense" approach that extends sensing and other means beyond DoD networks (OASD[NII]/DoD CIO, 2009). Caulkins (2009) proposes a "proactive self-defense" using sensors outside of U.S. boundaries to anticipate future attacks from abroad.[34] More recently Lynn (2010b) described an "active defense" approach, noting how the NSA has "pioneered systems that, using warnings provided by U.S. intelligence capabilities, automatically deploy defenses to counter intrusions in real time." These are similar concepts that potentially affect responses to intrusions into U.S. networks by adversaries seeking to exploit the broader commons that includes the Internet.

Levon Anderson (2007) conducted a department-by-department analysis to identify the federal agency best able to counter a cyber attack. His qualitative assessments tend to favor DoD/NSA leadership in countering state-sponsored cyber attacks. According to Anderson (2007), the NSA is the best-resourced (in terms of personnel and funds) and most operationally experienced organization with regard to cyberspace operations. A summary of Anderson's analysis appears in Table 2.

In fact, DoD deals daily with intrusions on its own networks by other nations. The U.S. Department of Justice also has operational experience with domestic cyber crime. A strength of DHS is its industry ties, as well as its mandate to protect the homeland from terrorist attacks; it is, however, the newest department.[35]

---

[31] To be complete, we must mention a counterargument best expressed by our colleague Mark Sparkman (2011): While DoD has formally declared "cyberspace" as a domain (see Appendix A), that concept is not universally accepted, particularly by the U.S. intelligence community, the Departments of Justice and State, and many others. One could argue that the Stuxnet operation was an intelligence operation and thus clearly "Title 50" in U.S. parlance—merely a covert activity and not a case of "cyberwarfare," which is a military activity undertaken to achieve military objectives.

[32] Caulkins (2009. p. 15) notes how this point is made in the *National Strategy to Secure Cyberspace* (2003), which states that "no cybersecurity plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly."

[33] An intrusion is only one step (a keystroke, perhaps) short of an attack.

[34] The legal and international norms regarding this are still up for discussion (Robinson, 2011).

[35] Melissa Hathaway (2011) points out a concern that "[w]e appear to be asking DHS to take on new cybersecurity roles and missions while it is establishing its basic core competencies. Is this reasonable? Do we want DHS to become a first party regulator?"

Table 2
Organizational Strengths and Weaknesses of Federal Agencies in Defending U.S. Cyberspace Infrastructure

Agency	Funding/ Budget	International Broker	Operational Experience	Technology/ Equipment	Private-Sector Ties	Legal Limits
U.S. Department of Homeland Security	–		–	–	+	+
U.S. Department of Defense/National Security Agency	+		+	+		Domestically: – Abroad: +
U.S. Department of State	–	+				–
U.S. Department of Justice	–		+	+		Domestically: + Abroad: –

SOURCE: Anderson, 2007.

NOTE: + indicates a strength. – indicates a weakness.

Title 10 and Title 18 of the U.S. Code limit DoD operations domestically. There is historical precedent for using federal troops on U.S. soil that points to the ability to use DoD in securing the homeland outside of wartime (e.g., federal troops in Little Rock to enforce school desegregation, relief following Hurricane Katrina, security after the Rodney King trial riots in Los Angeles).

Recently, the White House announced a strategy to further its partnerships with other nations to enable better cybersecurity (Schmidt, 2011),[36] an approach that forwards the goals of "diplomacy, defense, and development" outlined in the *International Strategy for Cyberspace* (2011). The concept of deterrence is also addressed in that strategy, though we do not discuss it in this paper.[37] However, Table 2 reflects the Department of State's prominent role in this area.

Current Organizational Boundaries Hinder Identification and Mitigation

Formal roles and boundaries in cyberspace, such as offense, defense, public, private, .mil, .gov, and .com, were all originally established for many good reasons (e.g., to protect individual liberties, to more efficiently organize government operations). For now, DoD focuses on the .mil domain, while DHS concentrates on the .gov domain and coordinates the critical infrastructure protection of private company networks (Waddell, 2010). But currently, these boundaries slow the "speed of chase" needed to police this global commons.

The ways in which the U.S. Code is written demand careful consideration of these restrictions. Who can prosecute the policing action is strictly governed (e.g., Title 50, which relates to war and national defense, compared with Title 10, which relates to the armed forces). Nonetheless, we argue that offensive action cannot be excluded as a means to maintain a robust

[36] This may be seen in the context of discussion as to whether NATO Article V power (an attack against one NATO member is an attack against all) should extend to cyberwarfare (Robinson, 2011).

[37] Specifically, the strategy includes a deterrence component by declaring,

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. (*International Strategy for Cyberspace*, 2011)

defense, but it is highly restricted, often requiring presidential permission. In summary, offensive activity is limited and controlled at best; at worst, it is simply prohibited for some of the most capable organizations. But it is a needed capability for defenders in other areas of the U.S. government.

For defense (i.e., cybersecurity), there is more opportunity for collaboration. The NSA works closely with U.S. Cyber Command to defend the global information grid and, as noted in this paper, the NSA has a formal agreement with DHS to assist with the .gov domain, among other activities (see Appendix C). What remains as a vexing question—as pointed out by Waddell (2010)—is whether the NSA should have an expanded domestic responsibility with regard to cybersecurity. Right now, it is constrained from monitoring network traffic within the United States. The NSA cannot directly conduct Title 10 attacks, though it can provide support to them (through various means).[38]

In summary, it will be difficult for a single U.S. organization to serve as the police force authorized to chase adversaries across cyberspace. Although that would be ideal to have such a capability that could meet the speed of cyber, it is equally unpalatable to most in a democratic society, particularly those concerned about privacy infringements.

There is no simple solution. Clearly, one challenge is how to best navigate within the important requirements and expectations of a democratic society that depends on cyberspace (for example, freedom of expression, right to privacy) against an enemy that has no boundaries and can act with impunity and disregard for norms and legal frameworks. In addition to national security implications, the continued breaches of private-sector data to acquire personal information illegally erodes privacy as well. Meeting cyberspace security obligations to defend against challenges like Stuxnet without losing or undermining the benefits that cyberspace brings is undoubtedly a highly complex task with no easy solution.

Recommendations

Congress is studying its options with regard to organizational assignments and new authorities to provide a comprehensive new approach to cybersecurity. The perceived shortfalls in the various departments, as outlined in Table 2, have motivated many proposed bills. Of the proposed legislative initiatives over the past five years, few have passed. Table 3 presents three examples. See Appendix D for a more complete list of cyber-related legislation introduced between January 2010 and April 2011.[39] Collectively, the bills call for the following:

- more cybersecurity awareness and standardized notification of breaches in the private sector (at the federal level)[40]
- more cybersecurity education and training
- a new cybersecurity coordinator position in the executive branch, DHS, or DoD

---

[38] A geographic combatant command cannot conduct war absent standard approvals. To conduct an attack, U.S. Cyber Command needs an executive order, just like any command (Sparkman, 2011).

[39] We note that treaties should not be overlooked as playing a role in cyber security. A coalition of treaty signatories could exert considerable pressure if a state were seen as committing or ignoring cyber attacks launched from its territory.

[40] Many states already have notification requirements. A complicating factor is if the breach involves personally identifiable information. That is a separate topic not covered in this paper.

- development, enforcement, or incentives for adherence to new cybersecurity standards or the study of such standards.

What is needed, at a minimum, is additional congressional action to grant new authorities that accomplish at least the following two goals:

- Enable substantially better collaboration among the agencies listed in Table 2 (as well as the private sector).[41]
- Grant *at least one capable organization* the authority to track cyber intruders, criminals, and other hostile actors in cyberspace with the same freedom of maneuver these adversaries enjoy. New authorities would be required, along with substantial revisions to the U.S. Code—a daunting challenge—and significant public debate.

These recommendations will require additional analysis and further development. However, as goals, they are essential to informing that process. Some of the proposals (listed in Table 3 and Appendix D) do seem to address the first goal, but none has yet addressed the second. This is due in part to privacy concerns and a legacy (in the United States) of a firm boundary between domestic law enforcement and intelligence agencies. Porche (2010) suggests a next step:

> Government intrusion into private affairs, even for reasons of the common defense, evokes an emotional response. . . . A first step requires an honest, public debate [that] calls into question the very firewalls between public and private sectors that are intrinsic to democracy.

Future Work

In terms of extensions of this paper, more research is needed on the proposed vision of a single agency or other construct to oversee a unified effort to protect U.S. interests in cyberspace. This would have to be achieved in a manner that accords with extant organizational architectures and corresponding responsibilities defined by U.S. Code.

Table 3
Examples of Proposed Legislation Regarding the Assignment of Federal Roles in Cyberspace

Bill	Introduced by	Purpose/Objective
Protecting Cyberspace as a National Asset Act	Sen. Lieberman	Create a White House cybersecurity office that reports to the Secretary of DHS on day-to-day matters.
National Cyber Infrastructure Protection Act of 2010	Sen. Bond	Establish a Senate-confirmed, presidentially appointed cybersecurity coordinator to be housed in DoD but reporting directly to the president.
International Cyberspace and Cybersecurity Coordination Act of 2010	Sen. Kerry	Establish a coordinator at the Department of State for cybersecurity issues to coordinate policy with other U.S. agencies, including DHS, DoD, and the U.S. Departments of the Treasury, Justice and Commerce, as well as the intelligence community and the private sector.

[41] It has been observed that The Patriot Act closed many of the integration and synchronization gaps in the CT realm that had grown up over the years. It has been suggested that some of these remedies might act as a model (Sparkman, 2011).

For the community at large, the "attribution" issue remains a vexing problem: How does one retaliate when it is so difficult to determine who is responsible for a given cyber attack? For now, one proposed answer is to try to anticipate the origin and preemptively mitigate an attack in the first place, through offensive techniques carried out by a very capable cyber force.

APPENDIX A

The Cyberspace Domain

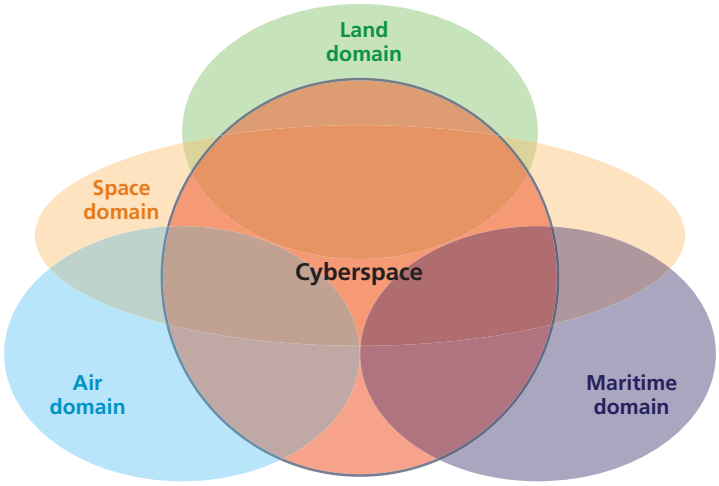
Cyberspace has joined the traditional domains of conflict, including land, sea, air, and space (see Figure A.1). DoD considers it to be a part of the so-called *information environment*, defined as the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (U.S. Joint Chiefs of Staff, 2011). Around the world, both the private and public sectors contribute to the information infrastructure.

Cyberspace itself has become something of a portmanteau word—that is, it brings together two separate ideas into one cohesive concept.

A number of trends have accelerated the transformation of cyberspace into a domain shared by citizens of the world:

- the move toward digitized information (voice, video, and data)
- the miniaturization of computing and data-storage devices that carry digitized information, coupled with low costs, which has fostered an explosion of increasingly networked digital devices
- the continued growth in wired and wireless networks and electronic systems, permitting access to systems that, until recently, may have been offline

Figure A.1
Cyberspace Today



RAND *OP342-A.1*

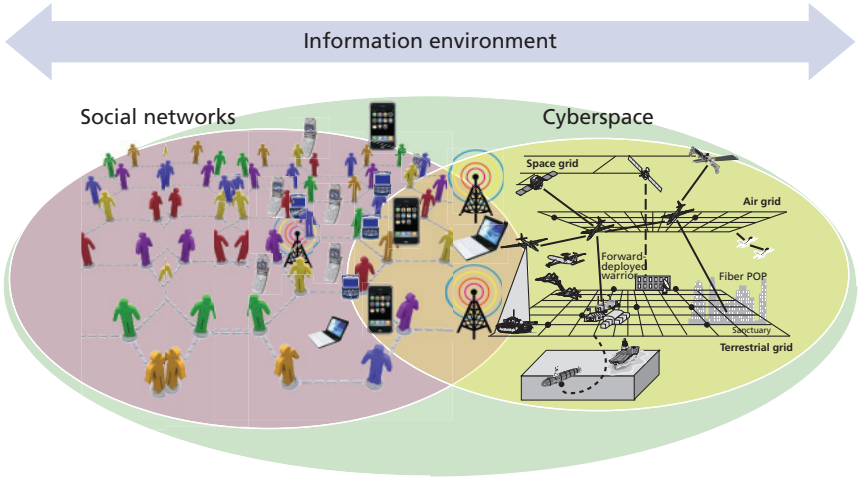
- the combined decrease in cost, increase in speed, and standardization of interoperating electronic systems, which not only make these systems more accessible to anyone but also increase the potential for exploitation.

These and other trends enable any government or state to use technologies that were once available only to developed countries with large defense budgets, though it should be noted that these capabilities simultaneously increase the exposure of those countries. Additionally, stateless individuals who were previously outnumbered or outgunned can now engage nations.

The presence and use of social networks in the information environment and the overlap with cyberspace are important developments. These networks are a growing venue for developing influence, as shown in Figure A.2. Internet-assisted social networking now influences daily sociopolitical events, as demonstrated by recent events in the Middle East and elsewhere, including Moldova, Iran, and even Pittsburgh.[1]

In summary, today's modern economic, political, and military systems depend more than ever on information and instructions that are generated in cyberspace nodes and transmitted across a vast network. Such reliance makes cyberspace a natural arena for conflict.

Figure A.2
Cyberspace and Social Networking



RAND *OP342-A.2*

[1] Cell phones, text messaging, and Twitter are believed to have played a crucial role in fostering the so-called Orange Revolution in the Ukraine by giving protestors a means to organize. Ultimately, the protests forced a recount of the general election. See Morozov, 2009; Goldstein, 2007; and Stack, 2009.

During Iran's so-called "Twitter revolution," Twitter feeds offered a constant stream of situational updates and links to photos and videos, all of which painted a portrait of the developing turmoil. According to news reports, when the Iranian regime began taking down these sources, the so-called e-dissidents shifted to email. See "Iran's Twitter Revolution," 2009.

During the 2009 G20 summit in Pittsburgh, protesters also leveraged Twitter. For example, Elliot Madison, an activist from New York City, was arrested after using Twitter to disseminate information about police activities to other protestors. Searches of his hotel room and, later, his residence in New York reportedly turned up laptop computers and emergency radio scanners used to track police movements. Madison and a fellow protestor were charged with hindering apprehension or prosecution, criminal use of a communication facility, and possession of instruments of crime ("Twitter Crackdown," 2009; Bankston, 2009; Goodman, 2009).

APPENDIX B

Worms

In this appendix, we provide background and definitions on computer worms, the threats they pose, and the vulnerabilities they can exploit.

Worm Attacks Are an Increasing Problem

A worm is an unwanted software program surreptitiously implanted on a computer that allows a remote user to control it. According to the U.S. Army Information Assurance Training Center (undated), "A worm is stand-alone software that does not require a host file to propagate. It doesn't even require human interaction; the computer merely needs to be turned on with its services running."

Worms in general are an increasing problem. To defend everyday computers (e.g., personal laptops and desktops) against worms, the typical course of action is to patch them with special "anti-malware" code for each newly discovered worm. This process must be repeated with every new version of the worm.

Agent.btz

Agent.btz was a worm that successfully compromised classified military computer networks in 2008. It was described in the open press in a *Los Angeles Times* article as malicious software, or malware, that was able to spread to any flash drive plugged into an infected computer and was specifically designed to attack military networks (Barnes, 2008).[1]

Deputy Secretary of Defense William Lynn, in an article published in *Foreign Affairs*, described the events as follows:

> It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. (Lynn, 2010b)

According to Lynn, it was "the most significant breach of U.S. military computers ever." This risk of spreading the malware to other networks prompted the military to ban the drives.

[1] As defined by the U.S. Army Information Assurance Training Center (undated),

> Malware is an acronym that stands for MALicious software and it comes in many forms. Generally speaking, malware is software code or snippets of code that is designed with malice in mind and usually performs undesirable actions on a host system.

Conficker

Conficker is a worm that may be amassing a massive "botnet" ("Conficker Worm Stealing Identities," 2009),[2] but its purpose is not yet clear. According to a Symantec report, it is a highly sophisticated worm that automatically propagates and shields itself from the effects of certain network defenses (Falliere, Murchu, and Chien, 2011). It is certainly capable of orchestrating a massive distributed denial-of-service attack (or even just an effective spam campaign).

The worm is smart: It is programmed to avoid IP addresses belonging to security companies, and it uses encryption to disguise what it is trying to do. The worm directs the machines it infects to communicate with each other so that the worm can update itself. Thus, it is constantly changing.

Like Agent.btz, one way of infecting hosts or computers is by means of insertion of removable drives (e.g., portable flash drives). Microsoft has offered hundreds of thousands of dollars for information on the authors of Conficker.

Worm Attacks Require Fast and Frequent Responses

The speed of the Conficker worm is shown in Figure B.1. Each mutation requires new software to protect against it. In this case, mutations occurred every month. A skilled adversary could create strains on a daily basis in response to patches. For these reasons, we conclude that the "speed of cyber" is uniquely fast within the realm of IT acquisition.

There are other reasons to acquire cyber assets rapidly, not the least of which is the need for offensive operations.

Zero-Day Exploits

A so-called zero-day exploit is any malware that exists but has not been detected and thus has no signature.[3] Stuxnet is an example of a zero-day exploit.[4] A form of network defense that relies on signatures to detect an attack is prevalent, so zero-day exploit attacks stand a great chance of going undetected long after damage has been done. This means that the need to react to a zero-day exploit, once it is eventually discovered, must be measured in hours or days because damage or the potential for damage will continue to accumulate.[5] By some accounts, the Iranian government took many months to discover and respond to Stuxnet.

---

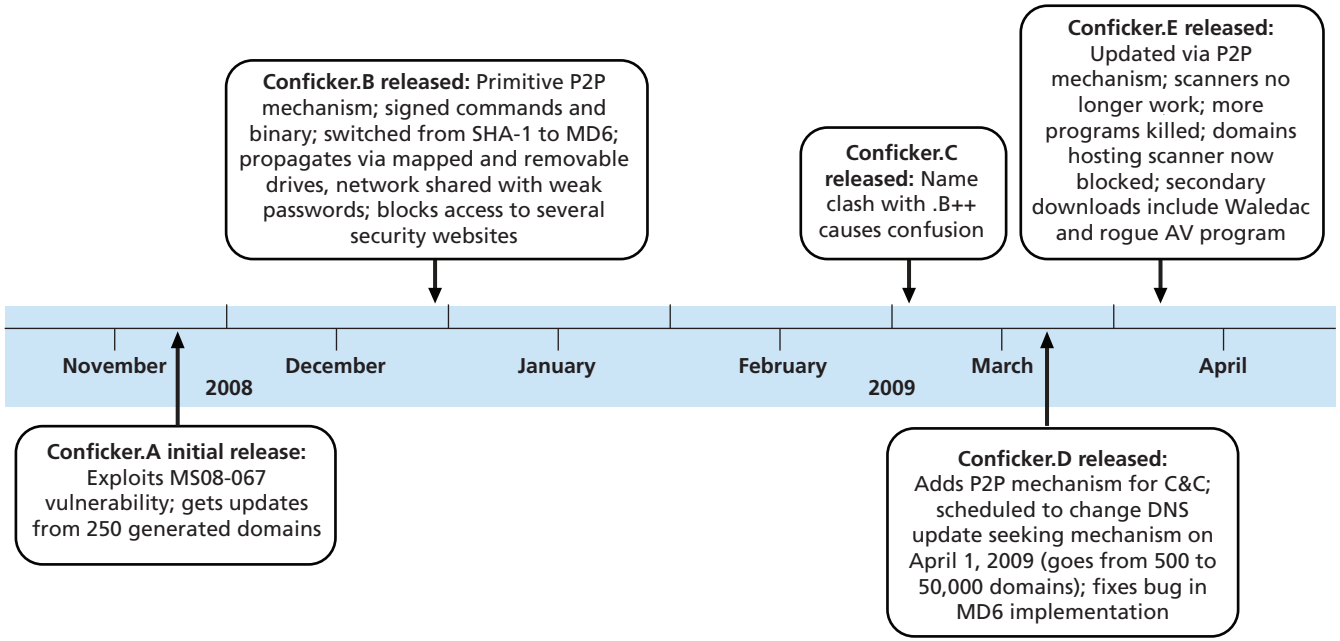
[2] Conficker is also known as a variant A of Win32.Donadup. Botnets, or bot networks, are made up of vast numbers of compromised computers that have been infected with malicious code and can be controlled remotely through commands sent via the Internet (Wilson, 2008, p. 5). They can be used by state actors or criminals to conduct a distributed denial-of-service attack, to produce spam, or for some other nefarious purpose.

[3] A signature is a recognizable pattern or characteristic of malware that allows antivirus software or other intrusion detection systems to be programmed to spot it.

[4] Specifically, it exploited four zero-day vulnerabilities (Falliere, Murchu, and Chien, 2011, p. x).

[5] The damage could be malware-guided physical destruction of a computer-controlled device or system or the loss of classified or sensitive data.

Figure B.1
Conficker Worm Progression



SOURCE: Conficker Working Group, 2009.
NOTE: P2P = peer to peer. C&C = command-and-control server.
RAND *OP342-B.1*

APPENDIX C

Einstein Intrusion Detection and Protection

The Einstein 1 and Einstein 2 programs are DHS-operated network monitoring efforts for federal government networks.[1] Einstein seeks to identify malware and disable it before it can harm government systems (Nakashima, 2009). Its sensors are installed where federal government systems connect to Tier 1 Internet service providers (Clarke and Knake, 2010, p. 164). Einstein 3 is the latest version and is being developed by the NSA for deployment by DHS. The military services have their own programs for network monitoring (Clarke and Knake, 2010, page 164).[2]

The use of Einstein or similar technologies by the government on its own or on the public's behalf raises the question of what the cyber privacy boundary should be.

Einstein and Privacy

With regard to Einstein and privacy, there are a few key considerations: (1) the use of deep packet inspection, (2) the networks on which it is done, and (3) the parties responsible for it.

Einstein 2 conducts "automatic *full packet inspection* of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology" (*Comprehensive National Cybersecurity Initiative*, 2010; emphasis added). Deep packet inspection involves examining all the content in a message, not just the packet headers (e.g., IP address) as many traditional firewalls do (Porter, 2005). Advocated as a promising cyber defense technology, administrators would have the potential to censor, data-mine, or eavesdrop on the contents of packets streaming over the Internet (Porter, 2005).

Who administers this technology is another aspect of this debate. Currently, DHS administers Einstein on government networks with the help of the NSA (*Comprehensive National Cybersecurity Initiative*, 2010). The level of DoD involvement in domestic cybersecurity is another real question, as evidenced by Einstein and increasing cybersecurity interdepartmental

[1] Einstein 1 "analyzes network flow information from participating federal executive government agencies and provides a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks" (DHS, 2008, p. 2). Einstein 2 is capable of "alerting the United States Computer Emergency Readiness Team (US-CERT) to the presence of malicious or potentially harmful computer network activity in federal executive agencies' network traffic." In addition, it "principally relies on commercially available intrusion detection capabilities" (DHS, 2008, p. 2). The programs are signature-based.

[2] Note that the U.S. Government Accountability Office (2010) has been critical of the DHS implementation of the Einstein programs.

collaboration between the NSA and DHS (Memorandum of agreement between DHS and DoD, 2010).

Again, cybersecurity must deal with the "global commons" nature of cyberspace within the bounds of privacy rights. The challenge here is focusing on how best to navigate within these privacy limitations against an enemy that has no boundaries.

Einstein and Intragovernmental Boundaries

The evolution of Einstein illustrates intragovernmental boundaries in practice. Einstein is the intrusion detection system for executive-branch networks (i.e., .gov domains) that monitors them for malicious activity. It is deployed by DHS but benefits from NSA developers, as mentioned earlier. The collaboration was established through a formal agreement between DHS and the NSA in late 2010 outlining the two agencies' exchange of

> personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. (Memorandum of agreement between DHS and DoD, 2010)

This intragovernmental relationship should enhance DHS's ability to use Einstein effectively by leveraging the NSA's threat-signature knowledge base and expertise (see *Comprehensive National Cybersecurity Initiative*, 2010).

APPENDIX D

Federal Cyber Legislation

Table D.1 presents a list of bills introduced in the House or Senate calling for

- more cybersecurity awareness (S. 813) and standardized notification of breaches in the private sector at the federal level[1]
- more cybersecurity education (H.R. 5966) and training (H.R. 76, H.R. 4507)
- a new cybersecurity coordinator position in the executive branch (H.R. 1136, H.R. 5548), DHS (H.R. 6423), or DoD (S. 3538)
- development, enforcement, or incentives (S. 21) for adherence to new cybersecurity standards (H.R. 174) or the study of such standards (S. 372, H.R. 6523).

[1] Many states already have notification requirements. A complicating factor is if the breach involves personally identifiable information. That is a separate topic not covered in this paper.

Table D.1
Federal Cyber Legislation

Date	Number	Short Title	Introduced by	Purpose/Objective
4/13/2011	S. 813	Cyber Security Public Awareness Act of 2011	Sen. Whitehouse (R.I.)	Promote public awareness of cyber security by requiring government agencies to improve publical reporting of cyber threats and breaches of security.
3/16/2011	H.R. 1136	Executive Cyberspace Coordination Act of 2011	Rep. Langevin (R.I.)	Establishes the National Office for Cyberspace, in the Executive Office of the President, to serve as the principal office for coordinating issues relating to cyberspace. The office would include the Federal Cybersecurity Practice Board, responsible for developing and updating information security policies and procedures. The bill requires the development of secure acquisition policies to be used in the procurement of information technology products and services, including a vulnerability assessment for any major system and its significant items of supply prior to development; includes requirements for agencies to undertake automated and continuous monitoring of their systems.
2/17/2011	S. 413	Cybersecurity and Internet Freedom Act of 2011	Sen. Lieberman (Conn.)	Authorizes DHS to require critical private-sector organizations to comply with protective measures in the event the president declares a "national cyberemergency." Establishes the Office of Cyberspace Policy in the Executive Office of the President. Authorizes the President to restrict Internet connectivity (to an extent) under limited circumstances if and only if an emergency is declared.
2/16/2011	S. 372	Cybersecurity and Internet Safety Standards Act	Sen. Cardin (Md.)	Directs DHS to conduct an analysis to determine the costs and benefits of requiring Internet service providers, communication service providers, electronic messaging providers, electronic mail providers, and others who provide a service or capability to enable computers to connect to the Internet to develop and enforce voluntary or mandatory minimum cybersecurity and Internet safety standards for users of computers to prevent terrorists, criminals, spies, and other malicious actors from compromising, disrupting, damaging, or destroying computer networks, critical infrastructure, and key resources.
1/25/2011	S. 21	Cyber Security and American Cyber Competitiveness Act of 2011	Sen. Reid (Nev.)	Provides incentives to improve the cybersecurity of the private sector and the capability of the U.S. government and the private sector to assess cyber risk and to prevent, detect, and robustly respond to cyber attacks against critical U.S. infrastructure.
1/5/2011	H.R. 174	Homeland Security Cyber and Physical Infrastructure Protection Act	Rep. Thompson (Miss.)	To enhance homeland security, including domestic preparedness and collective response to terrorism, by amending the Homeland Security Act of 2002 to establish the Cybersecurity Compliance Division and provide authority to DHS to enhance the security and resiliency of the nation's cyber and physical infrastructure against terrorism and other cyber attacks and for other purposes.

Table D.1—Continued

Date	Number	Short Title	Introduced by	Purpose/Objective
1/5/2011	H.R. 76	Cybersecurity Education Enhancement Act of 2011	Rep. Jackson Lee (Tex.)	Authorizing DHS to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs and for other purposes.
12/15/2010	H.R. 6523	Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (5 versions)	Rep. Skelton (Mo.)	Requires the Office of the Secretary of Defense to direct the DOD Chief Information Officer to work to achieve (1) the continuous prioritization of the policies, principles, standards, and guidelines developed under the National Institute of Standards and Technology Act, with agencies and offices operating or exercising control of national security systems based on the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of such incidents; and (2) the automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of Dod and the compliance of that infrastructure with such policies, procedures, and practices. Directs Office of the Secretary of Defense to develop and implement (by October 1, 2011) a strategy for assuring the security of software and software-based applications for major DoD systems, national security systems, and specified information systems; provide a report on the strategy; develop a strategy to rapidly acquire tools, applications, and other capabilities for cyber warfare for U.S. Cyber Command and report on the strategy; report on the DoD cyber warfare policy; submit progress reports on defending DoD and the defense industrial base from cyber events, such as attacks and intrusions.
11/17/2010	H.R. 6423	Homeland Security Cyber and Physical Infrastructure Protection Act of 2010	Rep. Thompson (Miss.)	Amends the Homeland Security Act of 2002 to establish the Office of Cybersecurity and Communications in DHS, to be headed by the Assistant Secretary for Cybersecurity and Communications. The office is to include (1) the U.S. Computer Emergency Readiness Team, (2) a Cybersecurity Compliance Division (established by this act), and (3) other DHS components with primary responsibility for emergency or national communication or cybersecurity.
9/29/2010	H.R. 6351	Strengthening Cybersecurity for Critical Infrastructure Act	Rep. Langevin (R.I.)	To establish the Executive Cyber Director in the Executive Office of the President; to clarify the authority of the Secretary of Homeland Security and the Executive Cyber Director with respect to critical information infrastructure policy creation, verification, and enforcement measures; and for other purposes.
7/29/2010	H.R. 5966	Cybersecurity Enhancement Act of 2010	Rep. Murphy (Pa.)	Authorizes the director of the NSA to establish a five-year pilot program to recruit highly skilled individuals who are pursing or have obtained a graduate degree in a field related to cybersecurity.

Table D.1—Continued

Date	Number	Short Title	Introduced by	Purpose/Objective
6/24/2010	S. 3538	National Cyber Infrastructure Protection Act of 2010	Sen. Bond (Mo.)	Establishes within DoD a National Cyber Center, headed by a director who reports directly to the President. The director's duties include (1) coordinating federal government defensive operations, intelligence collection and analysis, and activities to protect and defend government information networks; (2) acting as the principal adviser to the President, the National Security Council, and the heads of federal agencies on matters relating to the protection and defense of such networks; and (3) keeping appropriate congressional committees fully informed of the center's activities. Creates a voluntary, public-private partnership, the Cyber Defense Alliance, to facilitate the flow of information about cyber threats and the latest technologies between the private sector and government; creates a cybersecurity center housed at the U.S. Department of Energy that would allow critical private-sector entities, such as utilities, financial service firms, and power companies, to meet and share information on cyber attacks and best practices.
6/24/2010	H.R. 5590	Counterterrorism Enhancement and Department of Homeland Security Authorization Act of 2010	Rep. King (N.Y.)	Consolidates congressional oversight of DHS. Authorizes DHS to establish permanent U.S. Secret Service international field offices to enhance cybersecurity and the Secret Service's ability to combat cyber crime and counterfeiting of U.S. currency.
6/16/2010	H.R. 5548	Protecting Cyberspace as a National Asset Act of 2010	Rep. Harman (Calif.)	Establishes in the Executive Office of the President an Office of Cyberspace Policy to (1) develop a national strategy to increase the security and resiliency of cyberspace; (2) oversee, coordinate, and integrate federal policies and activities related to cyberspace security and resiliency; (3) ensure that all federal agencies comply with appropriate guidelines, policies, and directives from DHS, other federal agencies with responsibilities related to cybersecurity or resiliency, and the National Center for Cybersecurity and Communications (established by this act); and (4) ensure that federal agencies have access to, receive, and appropriately disseminate law enforcement, intelligence, terrorism, and other information relevant to the security of specified federal, military, and intelligence information infrastructure.
6/10/2010	S. 3480	Protecting Cyberspace as a National Asset Act of 2010	Sen. Lieberman (Conn.)	Create a White House cybersecurity office that reports to the Secretary of DHS on day-to-day matters.
6/4/2010	S. 3455	Department of Defense Authorization Act for Fiscal Year 2011	Sen. Levin (Mich.)	Limits the use of funds by Defense Advanced Research Projects Agency for operation of the National Cyber Range. Funds demonstration and pilot projects on cybersecurity.

Table D.1—Continued

Date	Number	Short Title	Introduced by	Purpose/Objective
4/26/2010	H.R. 5136	National Defense Authorization Act for Fiscal Year 2011 (5 versions)	Rep. Skelton (Mo.)	Expresses the sense of Congress that (1) cybersecurity is one of the most serious national security challenges facing the United States and that (2) it is critical for DoD to develop technological solutions that ensure its security and freedom of action while operating in the cyber domain. Directs the Secretary of Defense to study and report to the defense committees on tools to identify likely cybersecurity methodologies and vulnerabilities within DoD, as well as strategies and programs to deter hostile or malicious activity intended to compromise DoD information systems.
4/20/2010	H.R. 5081	Broadband for First Responders Act of 2010	Rep. King (N.Y.)	Amends the Communications Act of 1934 to increase the electromagnetic spectrum allocation for public safety services by 10 megahertz and reduce such allocation for commercial use by the same amount.
4/14/2010	H.R. 5026	GRID Act (5 versions)	Rep. Markey (Mass.)	Amends the Federal Power Act to direct the Federal Energy Regulatory Commission to issue rules or orders to protect critical electric infrastructure from cybersecurity vulnerabilities.
4/12/2010	S. 3193	International Cyberspace and Cybersecurity Coordination Act of 2010	Sen. Kerry (Mass.)	Establishes a coordinator at the U.S. Department of State for cyberspace and cybersecurity issues to coordinate policy with other U.S. agencies, including DHS, DoD, and the U.S. Departments of the Treasury, Justice, and Commerce, as well as the intelligence community and the private sector.
3/25/2010	H.R. 4962	International Cybercrime Reporting and Cooperation Act	Rep. Clarke (N.Y.)	Requires reporting on certain information and communication technologies of foreign countries; requires developing action plans to improve the capacity of certain countries to combat cybercrime and for other purposes.
3/23/2010	S. 3155	International Cybercrime Reporting and Cooperation Act	Sen. Gillibrand (N.Y.)	Requires reporting on certain information and communication technologies of foreign countries; requires developing action plans to improve the capacity of certain countries to combat cybercrime and for other purposes.
3/15/2010	H.R. 4842	Homeland Security Science and Technology Authorization Act of 2010 (4 versions)	Rep. Clarke (N.Y.)	Directs the Under Secretary for Science and Technology in DHS to (1) support research, development, testing, evaluation, and transition of cybersecurity technology, including fundamental, long-term research, to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from acts of terrorism and cyber attacks, with an emphasis on research and development relevant to large-scale, high-impact attacks; and (2) coordinate activities with the Under Secretary for National Protection and Programs and the heads of other relevant federal agencies.
2/23/2010	S. 3027	P2P Cyber Protection and Informed User Act	Sen. Klobuchar (Minn.)	To prevent the inadvertent disclosure of information on a computer through certain P2P file-sharing programs without first providing notice and obtaining consent from an owner or authorized user of the computer.

Table D.1—Continued

Date	Number	Short Title	Introduced by	Purpose/Objective
2/3/2010	H.AMDT.548		Rep. Matheson (Utah)	Amendment requires the National Science Foundation to study ways to improve detection, investigation, and prosecution of cyber crimes, including piracy of intellectual property, crimes against children, and organized crime.
1/26/2010	H.R. 4507	Cyber Security Domestic Preparedness Act	Rep. Rodriguez (Tex.)	Authorizes DHS to establish the Cyber Security Domestic Preparedness Consortium and training center to (1) provide training to state and local first responders and officials, specifically for preparing for and responding to cyber attacks; (2) develop and update a curriculum and training model; (3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response; and (4) conduct cybersecurity training and simulation exercises to defend against and respond to cyber attacks.

Bibliography

Albright, David, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*, Washington, D.C.: Institute for Science and International Security, December 22, 2010.

Alexander, GEN Keith, director, National Security Agency, and commander, U.S. Cyber Command, remarks at Center for Strategic and International Studies Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cybercom, Washington, D.C., June 3, 2010a. As of October 31, 2011: http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf

———, testimony before the Committee on Armed Services, U.S. House of Representatives, September 23, 2010b. As of October 31, 2011: http://www.stratcom.mil/speeches/2010/52/House_Armed_Services_Subcommittee_Cyberspace_Operations_Testimony

Ananthaswamy, Anil, "Internet Immunity System Promises to Defang Worm Attacks," *New Scientist*, Vol. 203, No. 2721, August 15, 2009.

Anderson, Levon, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers, and William O. Waddell, eds., *Information as Power: An Anthology of Selected United States Army War College Student Papers*, Vol. 2, Carlisle, Pa.: U.S. Army War College, 2007, pp. 105–122. As of October 31, 2011: http://www.carlisle.army.mil/DIME/documents/Information%20as%20Power%20Vol%202%20(web-final)[1].pdf

Assante, Michael J., vice president and chief security officer, North American Electric Reliability Corporation, before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House of Representatives, at the hearing "Security the Modern Electric Grid from Physical and Cyber Attacks," July 21, 2009. As of October 31, 2011: http://chsdemocrats.house.gov/SiteDocuments/20090721141526-32619.pdf

Baldor, Lolita, "Pentagon Gets Cyberwar Guidelines," Associated Press, June 22, 2011.

Balkovich, Edward, email to the authors, May 23, 2011.

Bankston, Kevin, "Man Arrested for Twittering Goes to Court, EFF Has the Documents," Electronic Frontier Foundation, October 5, 2009. As of October 31, 2011: http://www.eff.org/deeplinks/2009/10/man-arrested-twittering-goes-court-eff-has-documen

Barnes, Julian E., "Pentagon Computer Networks Attacked," *Los Angeles Times*, November 28, 2008. As of October 31, 2011: http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28

Broad, William, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 16, 2011. As of October 31, 2011: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Business Software Alliance, Center for Democracy and Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica, *Improving Our Nation's Cybersecurity Through the Public-Private Partnership*, white paper, March 8, 2011. As of October 31, 2011: http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf

"Canadian Researchers Uncover China-Based Electronic Spying Operation," Voice of America, March 30, 2009. As of October 31, 2011:
http://www.voanews.com/english/news/a-13-2009-03-30-voa66-68634007.html

Caulkins, Bruce D., *Proactive Self Defense in Cyberspace*, Carlisle, Pa.: U.S. Army War College, March 2009. As of October 31, 2011:
http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA494722

Chien, Eric, "Stuxnet: A Breakthrough," Siemens, November 16, 2010. As of October 31, 2011:
http://www.symantec.com/connect/blogs/stuxnet-breakthrough

Clarke, Richard A., and Rober Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, New York: HarperCollins, 2010.

The Comprehensive National Cybersecurity Initiative, Washington, D.C.: White House, March 2, 2010. As of October 31, 2011:
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Conficker Working Group, "Timeline," web page, last updated April 26, 2009. As of October 31, 2011:
http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline

"Conficker Worm Stealing Identities," United Press International, April 13, 2009. As of November 14, 2011:
http://www.upi.com/Top_News/2009/04/13/Conficker-worm-stealing-identities/UPI-39171239673271/

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, D.C.: White House, May 2009. As of October 31, 2011:
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

DHS—*see* U.S. Department of Homeland Security.

Dilanian, Ken, "Virtual War a Real Threat," *Los Angeles Times*, March 28, 2011. As of October 31, 2011:
http://articles.latimes.com/2011/mar/28/nation/la-na-cyber-war-20110328

Dockery, Stephen, "FBI Mum on Hacker Attack on Conn. Affiliate," *Boston Globe*, June 24, 2011. As of October 31, 2011:
http://articles.boston.com/2011-06-24/news/29699953_1_hacker-attack-website-fbi

Edwards, Marty, Idaho National Laboratory, and Todd Stauffer, Siemens, "Control System Security Assessments," presentation no. 2481, 2008 Siemens Automation Summit and User Conference, Chicago, Ill., July 2008. As of October 3,1 2011:
http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf

European Network and Information Security Agency, *Cloud Computing: Information Assurance Framework*, November 2009. As of November 21, 2011:
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

Falliere, Nicolas, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," version 1.4, Cupertino, Calif.: Symantec Corporation, February 2011. As of October 31, 2011:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

FBI—*see* Federal Bureau of Investigation.

Federal Bureau of Investigation, "National Cyber Investigative Task Force," web page, undated. As of October 31, 2011:
http://www.fbi.gov/about-us/investigate/cyber/ncijtf

Fulghum, David A., "Searching for Ways to Trace Cyber Attackers," *Aviation Week and Space Technology*, May 20, 2011.

Gates, Robert M., "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January–February 2009.

Goldstein, Joshua, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*, Cambridge, Mass.: Berkman Center for Internet and Society, Harvard University, December 2007. As of October 31, 2011:
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf

Goodman, Amy, "Watch What You Tweet," *Truthdig*, October 6, 2009. As of October 31, 2011: http://www.truthdig.com/report/item/20091006_watch_what_you_tweet/?ln

Gross, Michael Joseph, "A Declaration of Cyberwar," *Vanity Fair*, April 2011. As of October 31, 2011: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

Harris, Shon, *CISSP Exam Guide*, 4th ed., New York: McGraw-Hill, 2008.

Hathaway, Melissa, "Defining New Cybersec Roles for DHS: Creating a 24x7 Operational Center of Excellence," GovInfoSecurity.com, June 24, 2011. As of October 31, 2011: http://blogs.govinfosecurity.com/posts.php?postID=988

Infraguard, "About Infraguard," web page, undated. As of October 31, 2011: http://www.infragard.net/about.php

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, Washington, D.C.: White House, May 2011. As of October 31, 2011: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," fact sheet, Washington, D.C.: White House, 2011. As of October 31, 2011: http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

"Iran's Twitter Revolution," *Washington Times*, June 16, 2009. As of October 31, 2011: http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution

Libicki, Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009. As of October 31, 2011: http://www.rand.org/pubs/monographs/MG877.html

Lute, Jane Holl, and Bruce McConnell, "A Civil Perspective on Cybersecurity," *Wired*, February 14, 2011. As of October 31, 2011: http://www.wired.com/threatlevel/2011/02/dhs-op-ed

Lynn, William III, Deputy Secretary of Defense, "Remarks at Stratcom Cyber Symposium," transcript, May 26, 2010a. As of October 31, 2011: http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1477

———, "Defending a New Domain," *Foreign Affairs*, September–October, 2010b, pp. 97–108.

McCullagh, Declan, "FBI Taps Cell Phone Mic as Eavesdropping Tool," ZDNet.com, December 1, 2006. As of October 31, 2011: http://www.zdnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/150467

McGurk, Sean P., director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security, statement before the Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, U.S. House of Representatives, April 15, 2011. As of October 31, 2011: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McGurk.pdf

Memorandum of agreement between the U.S. Department of Homeland Security and the U.S. Department of Defense regarding cybersecurity, October 13, 2010.

Mitnick, Kevin, and William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Ind.: Wiley, 2002.

Morozov, Evgeny, "Moldova's Twitter Revolution," blog post, *Foreign Policy*, April 7, 2009. As of October 31, 2011: http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution

Nakashima, Ellen, "Cybersecurity Plan to Involve NSA, Telecoms: DHS Officials Debating the Privacy Implications," *Washington Post*, July 3, 2009.

———, "White House Reveals Cybersecurity Plan," *Washington Post*, May 13, 2011, p. A2.

National Council of Information Sharing and Analysis Centers, homepage, undated. As of October 31, 2011: http://www.isaccouncil.org/

National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, Washington, D.C.: White House, April 2011.

National Strategy to Secure Cyberspace, Washington, D.C.: White House, February 2003.

OASD(NII)/DoD CIO—*see* Office of the Assistant Secretary of Defense for Networks and Information Integration/U.S. Department of Defense Chief Information Officer.

Office of the Privacy Commissioner of Canada, "Just Deliver the Packets," undated. As of October 31, 2011: http://dpi.priv.gc.ca/index.php/essays/just-deliver-the-packets

Office of the Assistant Secretary of Defense for Networks and Information Integration/U.S. Department of Defense Chief Information Officer, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, Washington, D.C, August 2009. As of October 31, 2011: http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, D.C.: National Academies Press, 2009.

Peters, Katherine McIntire, "Information Insecurity," *Government Executive*, April 1, 1999. As of October 31, 2011: http://www.govexec.com/features/0499/0499s1.htm

Porche, Isaac, "Stuxnet Is the World's Problem," *Bulletin of the Atomic Scientists*, web ed., December 19, 2010. As of October 31, 2011: http://www.thebulletin.org/web-edition/op-eds/stuxnet-the-worlds-problem

Porter, Thomas, "The Perils of Deep Packet Inspection," Symantec, October 19, 2005. As of October 31, 2011: http://www.symantec.com/connect/articles/perils-deep-packet-inspection

Reed, Thomas C., *At the Abyss: An Insider's History of the Cold War*, New York: Random House, 2004.

Robinson, Neil, personal communication with the authors, June 27, 2011.

Schmidt, Howard, "Launching the U.S. International Strategy for Cyberspace," *White House Blog*, March 16, 2011. As of October 31, 2011: http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace

Shanker, Thom, and David E. Sanger, "Privacy May Be a Victim in Cyberdefense Plan," *New York Times*, June 13, 2009. As of October 31, 2011: http://www.nytimes.com/2009/06/13/us/politics/13cyber.html

Sparkman, Mark, personal communication with the authors, June 16, 2011.

Spillius, Alex, "US Could Respond to Cyber-Attack with Conventional Weapons," *Telegraph* (London), June 1, 2011. As od October 31, 2011: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/US-could-respond-to-cyber-attack-with-conventional-weapons.html

Stack, Graham, "'Twitter Revolution' Moldovan Activist Goes into Hiding," *Guardian*, April 15, 2009. As of October 31, 2011: http://www.guardian.co.uk/world/2009/apr/15/moldova-activist-hiding-protests

Steiner, Peter, cartoon captioned, "On the Internet, nobody knows you're a dog," *New Yorker*, Vol. 69, No. 20, July 5, 1993, p. 61.

"Twitter Crackdown: NYC Activist Arrested for Using Social Networking Site During G-20 Protest in Pittsburgh," Democracy Now! October 6, 2009. As of October 31, 2011: http://www.democracynow.org/2009/10/6/twitter_crackdown_nyc_activist_arrested_for

U.S. Army Information Assurance Training Center, "Information Assurance Fundamentals (IAF) Training, Lesson 6: Malware," undated. As of October 31, 2011: https://ia.signal.army.mil/IAF/IASOLesson6.asp

U.S. Department of Homeland Security, *Privacy Impact Assessment for EINSTEIN 2*, Washington, D.C., May 19, 2008. As of October 31, 2011: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

———, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*, Washington, D.C., March 23, 2011. As of October 31, 2011: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

U.S. Government Accountability Office, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, Washington, D.C., GAO 10-237, March 2010.

———, Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed, Washington, D.C., GAO-11-117, January 2011.

U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C., Joint Publication 1-02, November 8, 2010, as amended through September 15, 2011.

Waddell, William, "The DoD/DHS Cyber Lash-Up: Business as Usual or Government Expansion," *Dime Blog*, November 2, 2010. As of October 31, 2011: http://www.carlisle.army.mil/dime/blog/archivedArticle.cfm?blog=dime&id=141

Wilson, Clay, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Washington, D.C.: Congressional Research Service, RL32114, January 29, 2008.

Winter, Michael, "Iran's Leader Confirms Attack on Nuclear Computers; Top Cyberscientist Slain," *USA Today*, November 29, 2010. As of October 31, 2011: http://content.usatoday.com/communities/ondeadline/post/2010/11/irans-leader-confirms-attack-on-nuclear-computers-top-cyber-scientist-slain/1