Industry's Vital Role in National Cyber Security

James P. Farwell

The competing demands of economic recovery and protecting critical cyber infrastructure (CI) have heightened the need for stronger partnerships between the US government (USG) and private industry. Developing new technologies, strategies, plans, operations, tools, and techniques are essential to protect cyber security. How we meet this challenge has opened an important philosophical debate in the United States about the role of government and its relationship to private industry.

US Cyber Command chief Gen Keith Alexander has advised Congress that cyber threats to military and commercial sectors are growing and that criminals have exploited 75 percent of our nation's computers.[1] Intelligence and criminal threats have spotlighted discussion on how the military protects its assets, networks, and systems, and no one disputes the military's pivotal role in cyber security.

Yet, 90 percent of US critical cyber infrastructure is owned by the private sector.[2] Melissa Hathaway, who served as the cyber coordination executive for the Director of National Intelligence (DNI), has rightly pointed out that corporate and political leaders "appear to be paralyzed about meeting the needs for our cyber infrastructures and enterprises."[3] This current deadlock undercuts American security interests, and Congress must strike a balance between competing policy perspectives for cyber security. The dilemma is that earning a profit motivates industry, while protecting national security motivates the USG. Although often complementary, these agendas do compete. What is required is a confluent approach that removes legislative obstacles to stronger cyber security, forges robust partnerships between the public and private sectors, and better manages risk in the global supply chain. A review of current US strategy and the threat matrix is instructive in framing a new approach.

James P. Farwell is an expert in strategic communication and information strategy who has served as a consultant to the Department of Defense, the US Strategic Command, and the US Special Operations Command. He has three decades' experience as a political consultant in US presidential, congressional, and other campaigns. He has published numerous articles and *The Pakistan Cauldron: Conspiracy, Assassination and Instability* (Potomac Books, 2011).

The Current Strategy

A 2007 presidential directive ordered the Department of Defense (DoD) to protect its critical infrastructure.[4] The order endorsed a collaborative, coordinated effort to identify, assess, and improve critical infrastructure within the defense industrial base (DIB).[5] The DIB includes "the DoD, US government, and the private sector worldwide industrial complex with capabilities to perform research and develop, produce, deliver, and maintain military weapon systems, subsystems, components or parts to meet military requirements necessary to fulfill the National Military Strategy."[6] Most of the DIB is privately owned. It includes businesses of all sizes, including small, innovative companies that move rapidly and offer cutting-edge ideas that can be translated into usable products.

The Department of Homeland Security (DHS) holds responsibility for protecting civilian critical infrastructure and key resources (CIKR).[7] CIKR includes "assets, systems, networks, and functions that provide vital services to the nation," for which attacks or disruption could produce large-scale human casualties, property destruction, and economic damage as well as damage national prestige, morale, and confidence.[8] To help coordinate protection responsibility, the DHS devised a national infrastructure protection plan (NIPP).[9] In concept, the NIPP provides a unifying structure to integrate efforts to protect the CIKR into a single national program. The plan aims to balance resiliency with focused, risk-informed prevention and preparedness. Eighteen sector-specific plans (SSP) support the NIPP. These address efforts among local, state, and federal efforts, the private sector, and international organizations and allies.[10] Plans provide vision, coherence, and courses of action for a way ahead. But what must be done to more fully implement the current cyber strategy?

In July 2011, the DoD released its new *Strategy for Operating in Cyberspace*.[11] Five precepts guide it. First, by treating cyberspace as an operational domain, it seeks "increased training, information assurance, greater situational awareness, and creating secure and resilient network environments." Second, calling for "cyber hygiene" in security, it looks to strengthen the workforce and employ new operating concepts to improve security. Third, it recognizes that private-public partnerships form the foundation for an "active, layered defense." Fourth, it embraces international partnerships. Since cyberspace transcends traditional geographic borders, incidents may occur across national jurisdictions, and effective action requires multilateral cooperation among allies. The NATO 2020 report also calls for incorporating cyber defense into allied strategic thinking.[12] Finally, the strategy aims to catalyze civilian talent and ingenuity to spur new technology. It recognizes that entrepreneurs in small and medium-size companies often stand at the cutting edge in moving concepts from innovative idea to reality and scaled adoption.

The Emerging Threat Matrix

What is a cyber threat and how should that term be defined and addressed? One starts by distinguishing between cyber threats and cyber indicators. The distinction matters. Cyber experts Dan Auerback and Lee Tien suggest that a cyber security threat is what we guard against, while a "cyber security threat indicator" is the activity that allows private or public entities to monitor and execute countermeasures. They note that stealing passwords from a secure government server might be a threat, while a port scan to search for vulnerabilities is an indicator—a vague distinction. Legislative reform needs to clearly define each and address every aspect of cyber security.[13] Definitions need to embrace the notion that counterintrusion is self-defense and clearly define exploitation, counterexploitation, and self-defense tactics. Century Link's chief security officer David Mahon has well summarized the major cyber threats faced by the public and private sector.[14] They fall generally into four categories: nation-state intrusions (also known as "advanced persistent threat"); criminal, which extends to sophisticated organized crime; "hackivism"; and insider attacks.

Fast-evolving technology is altering the strategic implications for cyber capabilities, expanding and intensifying these threats. The world around us is changing quickly, reshaping the political environment. That affects strategic considerations. The Internet stands out as an emblem of this radical transformation. The global digital infrastructure, "institutions, practices and protocols that together organize and deliver the increasing power of digital technology to business and society,"[15] has reconfigured how business is conducted. Preparing for the next threat requires thinking ahead. Defensive strategies that worked before may prove obsolete if one attempts to win the next war by refighting the last one.

The threats are also new. Former assistant secretary of defense William J. Lynn has long worried about the impact of network destruction.[16] The Russian-backed denial of service attacks on Estonia and Georgia[17] and the assault on eBay and PayPal by the hacker group Anonymous illustrate that governments and companies are both vulnerable. The emergence of cyber weapons like Stuxnet, which impeded Iran's nuclear centrifuge program, opens a window to the future.[18] Initial reports suggested that assets of friendly nations, such as an Indian satellite, also sustained damage,[19] although doubts about that later arose.[20]

Critics of Iran cheered Stuxnet I. But Stuxnet II may target US or allied critical infrastructure. Blended attacks, employing cyber and kinetic weapons in combination, could zero in on military and civilian targets, destroying some while launching sophisticated penetrations of networks that control critical civilian infrastructure. The emerging political ecosystem in which new weapons are originating from nonstate parties, including criminal enterprises, unveils complicated and unpredictable scenarios.[21]

Concerns about Chinese cyber espionage and piracy (or, in obtuse national security jargon, "cyberexploitation") highlight another challenge. The US-China Economic and Security Review Commission has repeatedly warned that the Chinese are guilty of rampant cyber piracy—stealing intellectual property and trade secrets vital to US defense and to keeping it technologically competitive.[22] This concern is one element of a broader challenge, as rivals or foes employ multiple channels to acquire confidential and proprietary data. A 2012 report to the commission points to "collaboration between US and Chinese information security firms . . . over the potential for illicit access to sensitive network vulnerability."[23] What cannot be hacked may yet be obtained through legal acquisition from US companies. These concerns must be addressed as part of a broad strategy to protect our interests.

Human mistakes or errors in judgment challenge our most sensitive networks and systems, as Dr. James Peery of the Energy Department's Sandia National Laboratories warned the US Senate that we must "assume our adversary is in our networks, on our machines." Still, he noted, "We've got to operate anyway."[24] His fears are well founded. In 2008, hackers penetrated the Pentagon's classified Secret Internet Protocol Router Network (SIPRNET) when a flash drive loaded with "Agent.btz," a malicious code devised by a foreign intelligence agency, was left in a Middle East parking lot. Later, someone inserted it into a USCENTCOM laptop.[25] The incident infected computers and even the Joint Worldwide Intelligence Communication System, which carries top-secret information. The damage inflicted remains undisclosed.[26]

Lynn acknowledged that other penetrations remain undetected.[27] He considered the 2008 penetration an "important wake-up call" and a "turning point."[28] The Pentagon took remedial action, launching Operation Buckshot Yankee that led to banning the use of thumb drives[29] and creation of the US Cyber Command. Still, the incident proved how nettlesome cyber attacks can prove. Cleaning up this single problem took the Pentagon 14 months[30]—proof, one might argue, that private companies may prove more agile in coping with such crises and might have gotten the job done more efficiently.

The Pentagon recognized the problem as early as the 1990s. Solar Sunrise, a series of computer attacks in 1998 that targeted defense networks, led to intrusion detection systems on key nodes.[31] The incident confirmed findings derived from the 1997 Eligible Receiver exercise that had uncovered vulnerabilities in DoD cyber systems and demonstrated the increasing risks to US interests in cyberspace.

Individual attackers have underscored the potential for mischief. Over a decade ago, New Jersey programmer David Smith created "Melissa," a virus that used a Microsoft Word document sent as an e-mail attachment to infect classified US commercial networks, forcing Microsoft and Intel to shut down their e-mail servers.[32] The incident revealed that human beings are often the weak link in cyber security—recognition pivotal to the new US strategy.

At the same time, corporate vulnerability is growing. A Bloomberg survey of the utility, telecommunication, financial services, and health care industries revealed that technology managers in 124 companies—each with at least 10,000 workers—said they could double spending on cyber security and yet their networks would remain vulnerable.[33] An attack originating in China pirated intellectual property from Google.[34] Payments processor Global Payments reported a breach that affected 1.5 million credit card account numbers, forcing VISA to revoke its seal of approval from the company.[35] Mike Blake, chief information officer of the Hyatt hotel chain, commented, "If those guys can be penetrated, so can anyone else. So prepare yourself to be penetrated."[36] Sony Corporation has admitted that hackers accessed personal information on 24.6 million customers on a single online game service in an attack that compromised 100 million accounts.[37] Hackers have stolen data from 77 million Sony customers and compromised over 360,000 accounts at CitiBank.[38] Even highly sophisticated parties remain vulnerable. Worse, many companies remain unaware of hacking and theft.[39]

Stealthy foes can also corrupt hardware and software. Reportedly, Russia and China have probed the US power grid to identify vulnerabilities and have left behind software programs that may be deployed for disruption.[40] Concrete evidence of cyber mischief surfaced in Australia, where a disgruntled employee rigged a computerized control system at a water treatment plant and released over 200,000 gallons of sewage into parks, rivers, and the grounds of a Hyatt hotel.[41]

In a penetrating analysis of the cyber world, Heritage Foundation expert and author James Carafano points out the revolution that Internet technology has wrought. In unprecedented ways, he notes, a very few people can strongly impact masses of individuals.[42] He was writing about influencing crowd behavior, but his point holds for the threats small groups of individuals, acting alone or as state proxies, pose to critical infrastructure. Today one individual can change the way we think about the world and how we do business. At age 20, Mark Zuckerberg upended the way people communicate with one another in creating Facebook.[43] Sean Parker founded Napster and changed the music industry.[44] And over a decade ago, two Filipino computer programmers infamously devised the "I Love You" virus that caused over $5.5 billion in damages and infected more than 50 million computers.[45]

Not only existing networks or systems raise concerns. Microsoft's Eric Warner has cautioned that foes can "manipulate or sabotage systems during their design, development or delivery to determine or disrupt government functions."[46] Peery has labeled the information technology supply chain "a particularly insidious risk" and of "high consequence" to national security systems because of our widespread reliance on commercial-off-the-shelf (COTS) hardware and software technology that is increasingly produced, in whole or in part, by untrusted, non-US organizations. Unfortunately, the growing complexity of these systems also makes it economically infeasible to verify them thoroughly.

Insufficient attention has been given to technical approaches for mitigating supply chain risks. Counterfeiting and subversion of critical components in high-consequence DoD systems could have a devastating effect on our ability to project military power with confidence around the world. "Better methodologies and technologies are needed for assessing and managing supply chain risks."[47]

The Federal Bureau of Investigation's top cyber cop, Shawn Henry, minced no words about where we stand in the battle to fend off hackers.

"We're not winning," he told the *Wall Street Journal*. In his judgment, the current private and public approach is "unsustainable."[48]

The 2011 RSA Security case is illustrative from an industry perspective. RSA manufactures a two-factor authentication token, SecureID. These widely used electronic keys use a two-pronged approach to confirm the identity of the person trying to access a computer system. Their technology is used by many financial networks and defense contractors. Infiltrators breached and compromised the systems of US defense contractors, including Lockheed Martin, who fell victim to hackers using duplicates of RSA's SecureID tokens to penetrate internal networks. The event forced Lockheed to shut down all remote access to its intranet for at least a week.[49] The significance of the infiltration is manifest in the fact that Lockheed and RSA supply coded access tokens to millions of corporate users and government officials.[50]

The event cast into high relief the tension between private and public interests. Although RSA eventually disclosed the problem to customers,[51] critics blasted the company for putting its interest in earning profits and maintaining the commercial viability of its product ahead of the security concerns of customers.[52] It took a week before RSA briefed the press about the problem and much longer to reveal that the attack had compromised its technology. Critics argue RSA's behavior cost clients millions of dollars.[53]

The company finally made a formal disclosure on its 8-K filing to the US Securities and Exchange Commission.[54] Experts like Hathaway argue the commission ought to require companies to make timely disclosures and to take remedial action.[55] The public interest clearly supports Hathaway's position. Why did RSA not act sooner? The most obvious inference is that the company perceived its own interests in a different light. RSA has shown little remorse, and one wonders whether it worried more about its legal consequences than its customers. The challenge underscores the need for Congress to provide strong incentives for information sharing and legal immunity by encouraging manufacturers to make affected stakeholders aware of cyber threats.

The Debate on Legislative Reform

Most agree that stronger cyber security requires legislative reform. Unfortunately, Congress has deadlocked over competing philosophies about government regulation and information sharing. The divide reflects partly whether the debate is about national security or economic growth.[56] The official report to the Permanent Select Committee on Intelligence in 2012 that supported Rep. Mike Rogers' cyber security bill which passed the US House but faced a White House veto, concluded that "intelligence collection efforts can and should be provided—in both classified and unclassified form (when possible)—to the private sector in order to help the owners and operators of the vast majority of America's information infrastructure better protect themselves."[57] The committee's observation helps frame the challenges.

Although reform efforts in 2012 failed, the issues are important and will likely see renewed debate in the next Congress. Two proposals spotlighted the debate. Senators Joe Lieberman and Susan Collins introduced the Cyber Security Act of 2012 (CSA),[58] while Senator John McCain introduced the SECURE IT Act.[59] Examining the policies that underlie each proposal illuminates the debate on what reform makes sense and what stands a chance of passage.

Competing Legislative Proposals

The Cyber Security Act (CSA) of 2012. Strongly supported by the White House, the CSA took dead aim at companies deemed unwilling to invest resources into providing strong cyber security. It set up a mandatory regulatory scheme that required critical cyber-infrastructure companies to propose DHS-approved security standards or have standards imposed upon them. It directed the DHS to work with industry to assess the risks and vulnerabilities of critical infrastructure and to develop security performance requirements for "covered critical infrastructure."[60] Either relevant federal regulators with authority over a particular industry or the DHS itself would oversee this regime. White House cyber security chief Howard Schmidt insisted that cyber security standards were essential. "As long as there are weak links in the core critical infrastructure," he declared, "there's a risk for everybody."

CSA sponsors also considered the existing patchwork of regulatory authorities inadequate. Regulatory bodies like the Federal Energy Regulatory Commission (FERC) or the Federal Communications Commission (FCC) possess authority to compel action, but they comprise a diverse matrix. Many doubt they can provide strategic cohesion. Complicating matters, states share regulatory authority with parties like the FERC.

Critics insisted that the proposed scheme would unreasonably burden industry, choke innovation, and hurt competitiveness, while failing to improve cyber security. They argued that potential mandates would be costly and potentially unaffordable to many companies. Hitting legislative roadblocks, CSA sponsors amended the bill, arguing the ammendments would make regulation voluntary.[61] The amended bill sought to promote investment in cyber security research, establish public-private exchanges for information sharing, and promote what it characterized as voluntary regulatory practices by companies to secure computer systems in exchange for legal immunity for information sharing. The opponents were not assuaged.

Critics dismissed the amendments as a ruse. They argued that even in this form, the government, not the private sector, would adopt and promulgate all standards. They charged that the bill failed to consider the specific needs and economic interests of small businesses. They complained that the bill carved out technology products, including those manufactured in countries like China, exempting them from characterization as cyber infrastructure.[*] They argued that the provisions for giving security clearances to companies were too lax[†] and that the framework for sharing information under the bill meant more government bureaucracy by giving the DHS secretary unchecked authority to designate federal and nonfederal entities as cyber exchanges. The provisions on information sharing were considered complicated and likely to impede rather than encourage private industry to share information and impeded the government's ability to use cyber threat information provided by the private sector to prevent terrorist acts or catch spies.[‡] A coalition of business and civil liberty groups, including Fight for the Future and the Electronic Frontier Foundation, joined to help defeat the CSA. Business blasted the revised bill as still unduly burdensome to commerce and denounced the DHS as incompetent to supervise any regulatory scheme for cyber.[§] Civil liberties groups worried that the CSA provided a license to spy on web users, provided information gleaned to the USG, and claimed broad legal immunity for actions. Other critics lamented that the bill created a spying regime that enabled surveillance of any threat a company perceived to its network. For instance, the bill provided that a "cyber security threat" existed if a company concluded that a user was obstructing its networks and it authorized

[*] CSA, S 3414, Section 102(b)(5).

[†] CSA, S 3414, Section 102(b)(5).

[‡] CSA, S 3414, Section 704(g) and 104(c)(4).

[§] CSA, S 3414, Section 103(a), (b), and (g) drew fire as empowering the federal government to mandate standards.

blocking action to disrupt user action.[62] Skeptics felt this gave companies overly broad discretion. On the other side, supporters felt privacy groups had been appeased by eliminating the DoD's existing ability to get cyber threat information immediately and directly from the private sector.*

The SECURE IT Act. SECURE IT aimed to facilitate information sharing and assigned the DoD the lead on cyber security. It espoused the view that compulsory regulation was unnecessary, as companies had a vested interest in building and maintaining customer support by providing secure IT services. In the House of Representatives, SECURE IT was preempted by passage of the substitute Cyber Intelligence Sharing and Protection Act (H.R. 3523), sponsored by Rep. Mike Rogers.[63] Bearing certain similarities to SECURE IT, H.R. 3523 facilitated swapping cyber threat intelligence and information between "appropriate, cleared" private companies and individuals and the National Security Agency (NSA) and other government departments like the DHS.[64] The House-passed bill required the head of a federal department or agency that receives cyber threat information to share it first with the DHS. Only by request and DHS approval could that information be shared with other departments or agencies.[65] SECURE IT supporters criticized the proposal for unnecessarily inflating the role of the DHS at the expense of the NSA, the Department of Justice, the DoD, and other stakeholders. The Rogers bill proved a footnote after the White House made clear it would veto the bill. Thus SECURE IT stood as the alternative to the CSA. Perhaps not surprisingly, legislative deadlock killed 2012 reform, arguably a casualty of overreaching. The wiser legislative strategy would have been to enact legislation that addressed information sharing, where common ground might have been found, while delaying debate on the more controversial ideas for regulation.

Prominent Legal Obstacles to Stronger Cyber Security

While debate over whether standards for cyber security should be mandated or voluntary has occupied center stage, other prominent obstacles that require legislative action include (1) US antitrust and unfair business laws[66] and (2) privacy laws such as the Electronic Communications Privacy Act and the Stored Communications Act.[67]

*CSA, S3414, Sec. 703(a)(1). Instead, NSA and DoD agencies would be required to obtain such information from DHS-selected exchanges in "as close to real time as possible." Sec. 703(a)(2). Critics argued that these provisions would delay access to real-time cyber threats, including those from China, Russia, and Iran.

The RSA incident illustrates why information sharing and information protection among companies is vital to identify risks and vulnerabilities, counter cyber threats, and create databanks. Companies and government need access to what the other knows or learns. Uncovering errors or problems in software, especially when they may occupy a few lines of code in a product that contains tens of millions of lines, can be difficult. Detection of a vulnerability—a worm, virus, trapdoor, or other risk—as well as countermeasures a party may develop should be shared with other potential cyber targets. Viable cyber security strategies mandate that all parties act on an informed basis.

Equally, the government has a strong interest in ensuring that sensitive or classified information is closely held by appropriate parties. That interest must be balanced with the need to provide innovative entrepreneurs who develop cutting-edge technology access to the information needed to create solutions.

Antitrust Regulation. Companies fear the antitrust division of the Department of Justice and the Federal Trade Commission (FTC). Both watch for activity perceived as collusion that may lead to price fixing, abuse of market power, allocation of customers, and other anticompetitive activity. Their posture underscores another dimension in the tension between public and private interests. No one challenges the conceptual validity of antitrust or unfair-business laws. But the public interest in promoting anticompetitive practices embodied in those laws must be balanced against national security interests.

In practice, larger companies—staffed by top-notch attorneys—are able to manage the challenge of sharing relevant information without breaching the Clayton Act, Sherman Act, or unfair business practice laws. A lot of information sharing takes place among companies. For example, Century Link, one of the top Internet service providers (ISP), advised Congress that when it learns from third-party partners that customer computers are likely infected with malware that makes them part of a "botnet," it notifies customers and directs them to resources to help clean up the malware. It provides educational material, antivirus protection, firewalls, and parental controls. It works with stakeholders and industry partners on border gateway protocol (BGP) security to prevent accidental or malicious Internet route hacking.[68] Other industries engage in comparable information-sharing practices.

Large companies have the resources and sophistication to avoid illegal collusive activities, but smaller companies may lack that capacity. There is a solution, and Congress appears to recognize it. Narrowly drawn reforms can limit disclosure of risks, threats, vulnerabilities, and approaches to protection of information systems and personally identifiable information. That would enable information sharing and cyber security without undercutting a competitive marketplace.[69]

All three legislative proposals would have removed antitrust and FTC legal barriers to permit companies to monitor and defend information systems against cyber threats. Each allowed private companies to share cyber threat information,[70] and each prohibited the use of information shared to gain an unfair competitive advantage.[71]

Privacy and Confidentiality. Concerns that information sharing or disclosures may create legal liability for claims alleging breach of confidentiality or privacy are acute. These include potential claims for release of confidential information without prior consent. Information security—confidentiality, integrity, availability—is top of mind for many. Governments, the military, hospitals, and companies amass enormous amounts of information about employees, customers, products, and research and wish to protect it. Each proposal protects privileged or confidential trade secrets and commercial or financial transactions.

Still, industry experts argue that clear, fair, and predictable legal standards are lacking.[72] Ironically, all three bills pending before Congress contained safe harbors for information sharing about cyber security threats. SECURE IT offered the strongest. It exempted from civil and criminal liability private entities that use authorized countermeasures or cyber security systems; the "use, receipt or disclosure of any cyber threat information;" or "subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entities."[73] H. R. 3523 is similar but employed a good faith standard.[74] The CSA embraced a safe harbor, adding good faith as an absolute affirmative defense for sharing information about cyber threats, although as noted above, critics on the right and left found cause for concern with its information sharing provisions.[75]

The safe harbor provision within SECURE IT applied only to information actually related to cyber threats, as defined in the bill. The Rogers bill and the CSA are broader. They provided insulation for good faith disclosure of information[76]—language that is arguably an open invitation to litigation for violation of antitrust and the Electronic Communications Privacy

Act and the Stored Communications Act.[77] All bills protected against contrary state laws through a preemption rule.[78] All clearly intended a narrow exemption to remove obstacles currently posed by antitrust and unfair-business law for sharing cyber risks.

One step legislative sponsors might consider for the next Congress is to create a space on the Internet that invites iterative thinking, ideas, and suggestions from interested stakeholders. That may provide a useful forum to hammer out issues, critique different proposals, and forge solutions that address the real concerns legal barriers pose.

All three proposals sought to promote sharing classified and unclassified cyber security threat indicators with appropriate federal and nonfederal entities, although they employ different procedures to achieve that result.[79] The bills sensibly made exemptions for disclosures from the Freedom of Information Act (FOIA), ensured that disclosures waive no legal privilege, permit ex parte communications, and prohibited the government from using disclosed information in a regulatory proceeding.

What about forced disclosure of information? The CSA purported to render it voluntary except to prevent imminent crimes.[80] Critics argued the bill actually requires mandatory, not voluntary disclosure, as companies escape legal liability under antitrust or other laws only if they share risk information with the government. Private sharing affords no safe harbor.

One disaster to avoid is an exemption—which the CSA included—for computer software and hardware.[81] If one adopts this approach to regulation, why exempt the Internet from cyber security requirements, given its well-disclosed vulnerabilities?[82] In March 2012, the DHS reported there were 86 reported attacks on computer systems in the United States that control critical infrastructure,[83] factories, and databases. Ghostnet and other incidents underscore Internet vulnerabilities.[84]

And as information sharing pertains to critical infrastructure, one must ask: What constitutes critical infrastructure? Who makes that determination? The CSA empowered the government—led generally by the DHS acting in tandem with other agencies, like the Federal Energy Regulatory Commission which regulates power companies, to make that determination. An asset, network, or system qualified if damage could cause interruption of life-sustaining services, catastrophic damages to the United States, or severe degradation of national security.[85] These categories are too broad, and if this approach is adopted, they must be more precise.

SECURE IT would require federal contractors to inform the government about cyber threats and make it easier for regulators and corporations to communicate about threats.[86] Both that bill and the one adopted by the House shared a philosophy rooted in the policy judgment that facilitating voluntary information sharing between the federal government and private parties—including easing antitrust laws that restrict information sharing between private companies and offering legal protections to companies that act proactively to protect their networks—would create a more secure cyber infrastructure and protect consumer privacy without creating a new bureaucracy. Senator McCain has stated, "The only government actions allowed by our bill are to get information voluntarily from the private sector and to share information back."[87] The policies that his proposal reflects are rooted in the view that the DoD, the NSA, and US Cyber Command have excellent capabilities that could be utilized for civilian networks. The Lieberman proponents preferred the DHS, and that policy issue lent itself to practical resolution. But they were never able to show convincingly why giving the DHS the lead made more sense.

While the expertise of our national security entities should be leveraged to promote public-private partnerships, security requirements may limit what can be shared, with whom, or under what circumstances. Close engagement, coordination, and cooperation are required on a case-by-case basis to address that issue. While seeking information or intelligence from the government or other parties, companies need to recognize—and take responsibility for—financial and legal risks they incur in operating vulnerable networks.[88]

Robust Private-Public Partnerships

The NIPP rests upon a risk-management framework of cooperation and coordination between the private and public sectors. That enables both sectors to set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness.[89]

Among the key issues that must be addressed in forging robust public-private partnerships are (1) joint planning, (2) creating incentives for innovative public-private partnerships, (3) resolving who defends private industry against cyber attack, (4) balancing cost sharing between public and private sectors, and (5) developing a viable approach that authorizes government to reasonably share classified information on cyber security.

Joint Planning

Advances in technology are accelerating the "network speed" at which incidents occur, and this pressures decision makers to act more quickly. Joint planning between government and industry strengthens the ability of each to anticipate looming threats and counter immediate risks.

How acute is this challenge? Defense Advanced Research Projects Agency (DARPA) deputy director Kaigham J. Gabriel has warned the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities that in today's threat environment, cyber security systems take too long to build and may become quickly obsolete. Once built, they merely set the stage for the next requirement. "Shelf-life of cyber security systems and capabilities," he declared, "is sometimes measured in days. Thus, to a greater degree than in other areas of defense, cyber security solutions require that we develop the ability to build quickly, at scale, and over a broad range of capabilities. This is true for offensive and defensive capabilities."[90]

The quality and nature of technology for cyber attack or cyber exploitation is expanding. "Computing, imaging, and communications capabilities that, as recently as 15 years ago, were the exclusive domain of military systems, are now in the hands of hundreds of millions of people around the world," Gabriel stated.[91] Nearly a dozen countries are producing electronic warfare systems. Many use mostly COTS technology. Decades ago a new system was produced every 10 years. Today, one is produced every year to year-and-a-half.[92] In testimony before Congress, Dr. James Miller pointed out that DoD acquisition processes require an average of 81 months to make new computing systems operational: "That means by the time they are fielded, they are already three to four generations behind the state of the art. We are working to get cycles of 12 to 36 months as opposed to 7 to 8 years."[93]

The military equips itself to protect its own assets, systems, and networks. Joint planning can help enable the defense industrial base to leverage that expertise in establishing a cohesive policy framework to forecast and meet challenges. Adopting this approach will force interested parties to focus on key questions: What priorities should govern planning? Where should capital investment be focused? How should industry and the government, each of which bears responsibility for security, allocate costs and responsibilities? What are actionable requirements to make cyber infrastructure as secure as possible? Where do we acquire the knowledge vital to making informed judgments in answering those questions?

Smart planning for cyber security is an iterative process. It entails asking the right questions, developing information needed to ensure the right questions, and conducting progressive analysis through public-private engagement. From a public perspective, government can encourage business to invest in security measures that exceed their narrower business concerns. From a private perspective, industry may gain access to expertise it lacks, along with a greater comprehension of its own responsibilities. Too often industry expects government to do all of the heavy lifting for cyber security. Yet, the obligations flow both ways.

Industry is more supple in developing and testing new products. Industry better generates innovative ideas and cutting-edge solutions. Industry owns and operates most of the critical infrastructure, affording it a better understanding of CIKR assets, systems, networks, and facilities. It can move more quickly to reduce risk and respond to incidents. DARPA has recognized through programs like Cyber Fast Track (CFT), which taps into a pool of nontraditional experts, that smaller and medium-sized companies are leaders in innovative technology and has adjusted its funding accordingly. Over the last 12 months, it has made 32 awards to private companies—84 percent of them small companies and performers who have never done business with the government before.[94] Gabriel astutely noted that it is vital to expand "the number and diversity of talent contributing to the Nation's cyber security."[95] The philosophy embraces the far-sighted view of looking to companies that take risks to create new ideas in comparison to larger organizations that by emphasizing greater adherence to established procedures or protocols may prove less adept at creating new products. DARPA's philosophy rightly stresses collaboration between government and industry.

James Peery of the Sandia National Laboratories seconds that view. In 2012 he advised the Senate Armed Services Committee that the federal government needs a new strategy that coordinates investments across government and that taps into expertise offered by academia, government, private-sector, and military users.[96]

In the United States, the public and private sectors already work together in many ways. The DHS National Coordinating Center enables operational and collaborative partnerships. The Communications, Security, Reliability and Interoperability Council (CSRIC) provides an effective vehicle for providing recommendations to the FCC.[97] The FBI's Domestic Security Alliance Council (DSAC) is a strategic partnership between the FBI, DHS, and the private sector to ensure effective exchange of information to keep the nation's critical infrastructure safe, secure, and resilient.[98] The National Cyber-Forensics Training Alliance (NCFTA) serves as a conduit between private industry and law enforcement to fight cyber crime.

Malware pandemics, such as the Conficker computer worm, underscore the need. Conficker targeted Microsoft's Windows operating system. First detected in November 2008,[99] it exploited flaws in Windows software to co-opt machines and link them to a remotely controlled virtual computer—a botnet. Conficker generated strong cooperation among industry, academia, and government. Collaboration grew to more than 100 level-one domain operators and kept Microsoft in daily touch with the Internet Corporation for Assigned Names and Numbers (ICANN) and governments. It also exposed legal challenges. In some countries, contractual barriers and antitrust laws had to be addressed.[100]

Success proved elusive. Conficker's creators have neither been identified nor caught, although in June 2011, Ukraine authorities working with the FBI arrested 16 hackers in Kiev who used Conficker to seal $72 million from bank accounts.[101] Conficker is a warning to those who flinch from strong public-private collaboration. There was more success in fighting DNS (Domain Name System) changer malware, which enables criminals to control user DNS servers and thus what sites the user connects to on the Internet. Criminals could cause an unsuspecting user to connect to a fraudulent website or interfere with a user's online web browsing.[102] More than 4 million computers were infected. Industry provided critical insights into the information environment, helped identify infected computers, and offered remedial action. The FBI is developing evidence and is prosecuting six Estonian nationals arrested and charged after a two-year operation.[103]

The response to these threats underscores that public-private engagement can be effectively achieved, illuminating the path to defense against cyber attacks. It also supports notions of active defense—which remains ill-defined but should include preemptive action, carefully limited and permitted without a structured policy framework—and for offense. Neither the United States nor other nations have released their offensive doctrine and/or descriptions of capability. What is clear is that the developing technology is providing the operational flexibility to maneuver in the cyber domain and to harmonize resources and capabilities within a coherent systematic strategy that permits the achievement of operational aims despite the opposition.

Forecasting the future can be a fool's errand. What we know is, as much as possible, we must look over the horizon. New technologies will produce new threats. These require evolutions in strategic thinking as well as technical and operational capabilities. Developing vital capabilities, tools, and weapons requires a joint effort between government and industry that capitalizes on the strengths of each.

Nothing underscores that more than the looming development of neuro-cyber weapons. New generations of these will enhance situational and strategic awareness, increasing the ability of humans to absorb, process, and project increasing volumes of data that could overwhelm individuals. Amplifying our ability to collect information and intelligence and properly analyze it will deepen situational and strategic awareness. Crises require humans to digest large volumes of data at a very high rate and to act on that data in a timely manner.[104] Some developments will be technical. Others entail revolutionary developments in medicine. Drugs like Ampakine CX717 may prevent harmful effects of sleep deprivation and enhance attention span and alertness.[105]

DARPA is developing cognitive technology that enables interactive monitoring to facilitate command and control of troops on the ground. These will help detect when an individual has physical limits to operate effectively or loses situational awareness. Robotic prostheses will replace body parts—enhancing capabilities to function in cyberspace—much as pacemakers or artificial legs now do so in medicine. Robotic orthotics will extend human performance.[106] These will improve cognitive skills through sensory substitution and enhancement. Next-generation computers will teach themselves, monitor information, and perform other tasks that augment the human brain. The trend is finding ways to expand distributed situational awareness by extending the human body, brain, and senses.[107]

These developments will enable the military to conduct cognitive hacking and both military and civilian entities to defend against it.[108] Tax incentives for private industry—which should not have to depend entirely upon entities like DARPA to support new technology, ideas, and products—should be an integral element of strategic thinking. They will help forge cyber strategies for offense or defense that entail tactics such as creating deception, distraction, distrust, and confusion. These tools may be integrated into combined arms strategies to prevent, detect, or interdict cyber security challenges—and to pursue active defense or offensive strategies essential to national security. They can be used strategically or tactically for things like PSYOPS to create operational shock in cyberspace—a tactic that may be used to influence, recruit, intimidate, or surprise.[109]

Incentives for New Partnerships

The ability of the private and public sectors to leverage the strengths of one another to create both new spaces for creative thinking and to spur innovation affords a key incentive to promote these relationships. That synergy will produce better strategic thinking and strong policy frameworks. It will also—and this addresses the core of Kaigham's concern—increase the rate at which innovation takes place. New knowledge is produced every day. It remakes the world and reshapes the political and information environment and the cyber domain. It accentuates the importance of some things, while rendering others obsolete.[110]

DARPA has already recognized this challenge and is moving toward providing more grants to small and medium-size entrepreneurial companies who can meet that need. The DoD and the NSA need to become more flexible in easing access and clearances to companies and their employees to make possible exchange of information and the symbiotic partnerships that will enable public-private partnerships to flourish.

Yet, we should not rely upon DARPA or other government grants to spur innovation and new technology. Providing tax incentives for new technology, products, and innovation would spur development and make the investment of capital more worthwhile. Defining goals and offering appropriate prizes—financial and other—offers a different approach that could yield tangible results. Engagement between companies and the government to ascertain what can most strongly encourage companies to act proactively would be productive.

Where all of these developments will lead is tantalizing. The future offers opportunity and warning. The possibilities currently within our reach would have astounded populations and planners of earlier eras. Clarke's Third Law holds that any sufficiently advanced technology is indistinguishable from magic. Future developments may only seem like conjuring, but the wonders that they hold will continue to astound. That is the perspective in which thinking about our cyber strategy needs to proceed. Collaboration and coordination that mobilizes and recruits the most imaginative talent from government and the private sector underscores the value of working together in developing joint policy frameworks and concrete action.

Who Defends Private Industry against Cyber Attack?

A joint policy framework is essential to forging a strategy to protect industry in real time against cyber attack or cyber exploitation. The challenge raises thorny issues. The DoD has made clear it will defend against attacks. More recently, it is embracing the notion of "active defense" to counter asymmetric threats. As William Lynn put it, "In this environment, a fortress mentality will not work. We cannot hide behind a Maginot line of firewalls . . . our defenses must be active."[111] He has noted that in cyber, milliseconds can make a difference. In that view, the Pentagon has embraced a defensive system with three overlapping lines of defense. Two, based on commercial best practices, are ordinary hygiene—keeping software up to date and firewalls up to date—and the use of intrusion-detection devices and monitoring software to establish a perimeter defense. The third is protecting critical infrastructure, including civilian infrastructure.[112]

That does not answer the question of what one means by an active defense or whether or how private critical infrastructure can mount it. Does it afford a right of hot pursuit? Does it embrace preemptive action? Who has, or should have, the authority to make decisions in mounting an active defense for national security incidents? The issue remains unresolved. One industry leader sees passive defense as reliance upon firewalls, intrusion-detection systems, and hygiene, while active defense means working "actively"—in concert with other parties to identify, intercept, and block attacks. That is a plausible explanation but represents a less aggressive view than that held by many who focus on defending military assets, networks, and systems.

The bottom line is: joint planning between government and industry is essential in thinking through who a company—a financial institution, utility, or other private party—can summon for help or what action it may legally or practically take to actively defend itself. The idea that companies should collect evidence and turn it over to proper law enforcement authorities may be useful down the road for prosecutions but fails to answer the critical question of how, beyond passive defenses like firewalls, one stops an attack or whether preemptive activity is permissible—and if so, under what guidelines?

The Computer Fraud and Abuse Act makes it a felony to intentionally access a computer without authorization and cause damages of $5,000 or more.[113] A foreign attacker may not be able to capitalize on that, but the Justice Department's responsibility is to enforce the law as written. And what happens if the attack originates in the United States? Does that not compound the problem? Industry currently lacks legal guidance—and recourse—for countering a real-time attack.

A joint public-private policy framework, augmented by legislative reforms that authorize desired strategies, is vital as this nation forges viable strategies that protect, as much as possible, its critical cyber infrastructure.

Balancing Public and Private Interests in Allocating Costs and Sharing Information

Who should bear the cost of continuous upgrades to cyber security? How should such decisions be reached? The answer lies in balancing regulation and volunteerism as resources and interests vary. Larger firms focus on protecting physical, human, and cyber assets. They can more easily bear costs. That begs the question of what security standards should be satisfied or who should formulate them—industry or the government? Smaller companies face stiff challenges as capital requirements may be steep. No single formula applies across the board. A key challenge is, while private business owns 90 percent of critical infrastructure,[114] no USG department possesses the authority to compel companies to meet security performance requirements.

The balance requires information sharing, engagement among DIB partners, and trust.[115] There are competing views on how to surmount this challenge. The approach embraced by SECURE IT and the House bill argues that the market and corporate self-interest in keeping customers satisfied will force companies to take proper measures to voluntarily protect themselves.

No solution is perfect, but what is required is strong engagement and partnership between public and private parties, keyed to specific sectors within industry and the government, to strike a workable balance.

While demand for cyber expertise greatly exceeds the supply,[116] top-tier places like Sandia National Laboratory recruit aggressively. Sandia will pay for a master's degree and support new recruits with 75 percent of their salary while they attend school fulltime in exchange for two years' service. There is intense competition for their knowledge and skills. Private companies often offer 50-percent higher salaries and benefits. So far, places like Sandia have been able to retain much of their workforce, and that is to everyone's benefit.[117]

The government offers a reservoir of talent, experience, and unique expertise. Places like Sandia offer innovative hands-on computer security programs, skill refreshing, and continuous learning. The government better understands countermeasures and best practices to address risks and vulnerabilities, and the private sector cannot match its intelligence-gathering capacity. All these actions benefit industry—which for its part bears the burden of taking active steps to protect its assets, systems, and networks. Melissa Hathaway offers a practical way forward in addressing this challenge: "DoD and the DNI have the authority to make the policy decision to declassify or 'write for release' to release vital information to a broader user community. That will greatly facilitate private-public information sharing and protection of critical infra-structure."[118]

A key challenge is enabling access to classified information among private-sector parties. The prevailing view would limit information sharing to individuals who possess appropriate security clearances, on a basis consistent with protecting national security. Congress is considering ways to enable cyber security providers, protected entities, or self-protected entities eligible for a clearance to obtain one if they show they are able to appropriately protect classified cyber threat intelligence. What is needed is for parties like the director of national intelligence or other responsible federal entities to work closely with private parties, flexibly taking into account private-sector innovation, corporate information sharing, and security best practices. Close engagement is required to establish realistic procedures that enable each side to access the expertise of the other. One way to achieve this may be to grant a temporary clearance for specific projects.[119]

Securing the Defense Industrial Base Supply Chain

The 2011 strategy recognizes that we have to manage supply chain risks. In protecting against supply chain vulnerabilities, the United States leans toward a combination of creating a secure pool of selected vendors and, for the broader commercial sector, identifying key assets and controls to assure the integrity of products, testing to mitigate threats, and using trusted companies who use processes like those described in SAFECode.[120] This approach addresses various sources of risk: (1) supplier issues such as the ability to keep costs low and manage inventory levels, managerial and decision-making skills, and overall quality; (2) supply chain collaboration risks raised by supplier firms, logistics firms, and improper collaboration along the supply chain; or (3) uncontrollable events or natural disasters, legal liabilities, market price increases for raw materials, and technology changes.[121]

Employment of carefully selected and screened indigenous manufacturers for sensitive products is one step. There is a compelling reason for countries to build a series of verifiably secure computer and communication systems. Setting specific technical standards and requirements that products and components must meet is important. Yet, these represent partial solutions.

One must be realistic about capabilities. Managing the risk in assuring security in the cyber supply chain can be challenging for private companies. Many companies lack the resources to verify product security. Managing supply chain risk requires active joint, government, and private coordination, trust, and partnership with continuous, vigorous, informed engagement from both sides. No single formula will suit every aspect of the private sector or government. That mandates a flexible, adaptable approach.

At least five confluent strategies make conceptual sense. Yet, it bears stressing—extensive engagement between government and industry is vital. Each offers particular strengths and assets in implementing these strategies. It is possible to establish a finite number of absolutely secure installations. But for most installations, these mitigate but do not eliminate risk. Aspects of the first four have received wide comment:[122]

1. Ensure Transparency

We should work to ensure vendors who supply components or finished IT products provide transparency as to design, production, assembly, acquisition, quality control, assurance of a trusted workforce, record-keeping, traceability within the supply chain,[123] transportation, use of authentication technology, and their own security safeguards.

2. Maintain Continuous Monitoring

Companies or government departments or agencies need to continuously monitor vendors and products to ensure products are secure from viruses, worms, or other vulnerabilities. Although this can be a logistical challenge, it is critical and will help ensure vendors institute proper safeguards. Conversely, government and commercial organizations need to develop and implement policies that prevent counterfeit parts from entering the supply chains.[124] The Department of Commerce and the Office of Technology Evaluation have offered recommendations to help ensure effective monitoring.[125]

3. Provide Incentives for Security

The private sector works well when presented with incentives to perform. While the threat not to do business provides any government or company with leverage to force vendors to ensure the security of their products, incentives tailored by different parties to vendors or products can pay off.

4. Establish a Database of Trusted Vendors

The United States and its partners should establish a database of vendors deemed trusted and reliable. The National Vulnerability Database provides and tracks vulnerability data for commonly used operating systems and applications, including open source, but it does not identify vendors.[126] It is vital to create fair, clear, and predictable rules and procedures for listing vendors and a workable procedure through which vendors denied a place can in a practical manner lodge an appeal and secure fair and impartial administrative adjudication. Collaterally, government agencies should have authority to refuse to deal with companies deemed unwilling or unable to counter supply-chain risk. Kathryn Stephens has sensibly recommended making the supply chain a part of the overall US cyber intelligence and cyber security strategy and setting up an organization that can handle reports of counterfeit products.[127]

5. Strengthen the Rules Governing the Committee on Foreign Investment in the United States (CFIUS)

Established in 1975 by Pres. Gerald Ford's Executive Order 11858, the CFIUS is an interagency committee of the USG that reviews the national security implications of foreign investments in US companies or operations. Chaired by the secretary of the treasury, it includes representatives from 16 departments and agencies. Companies involved in acquisitions by a foreign firm are supposed to voluntarily notify the CFIUS, but it can initiate reviews on its own. It has looked at restrictions on the sale of advanced computers to a long list of foreign recipients, ranging from China to Iran.[128]

We need to strengthen the law requiring mandatory disclosure to the CFIUS of proposed foreign investments in technology companies by nations that the White House deems an "intelligence risk." The CFIUS should be required to investigate whether such acquisitions might compromise security.

The CFIUS has exerted its authority in cases involving Huawei Technologies, a mammoth Chinese telecommunications company that has been charged with engaging in corporate espionage against Western firms.[129] US security requirements mandate a more active role.

What nations cannot pirate directly may prompt them to seek access in more indirect ways—and potentially enable those deemed to be intelligence threats to covertly modify technology ostensibly owned by a US manufacturer. For example, China's aggressive strategy to ferret out and seize US technology as well as trade secrets is manifested in parallel ways. It stands accused of cyber piracy. Others point to different strategies that pose risks to US manufacturers—and by extension, to IT security.

Dr. Ron Hart, co-author of the Technology Transfer Act of 1986, advises many emerging technology companies and is recognized as one of the top clean-tech alternative energy analysts in the United States. He reports that in the last six months alone, Chinese emissaries have approached these companies with an offer to invest venture capital in exchange for a minority stake of 20 percent to 30 percent of the corporate valuation. The Chinese employ a greatly inflated valuation compared to normal American venture capital assessments as an inducement to accept the offer. The structure of the offer is always the same. The Chinese require two board seats as well as the right to manufacture and distribute products in the People's Republic of China. US companies such as Cisco and Motorola that have located their manufacturing facilities in China have found their technology pirated.[130] It is a clever strategy and works in tandem with cyber piracy.

Conclusion

We need to move expeditiously but smartly to minimize cyber risks and vulnerabilities to critical infrastructure for both government and industry. To strengthen cyber security, we must remove legislative obstacles, develop partnerships between public and private interests, and expertly manage global supply chain risks. Government can work with the private sector in ways that offer strong incentives for the private sector to protect its own interests and that of the nation. The challenges posed by state and nonstate actors create a real and present danger that must be confronted. The sooner the better. SSQ

Notes

[1] "Statement of Gen Keith B. Alexander, commander, US Cyber Command, Hearing on National Defense Authorization Act for Fiscal Year 2012, Committee on Armed Services, US House of Representatives, 16 March 2011," 4, http://www.fas.org/irp/congress/2011_hr/cybercom.pdf.

[2] Richard Weitz, "Global Insights: The DHS' Cybersecurity Logjam," *World Politics Review*, 10 April 2012, http://www.worldpoliticsreview.com/articles/11827/global-insights-the-dhs-cybersecurity-logjam.

[3] Melissa E. Hathaway, telephone interview, 3 August 2012.

[4] "Homeland Security Presidential Directive 7: Critical Infrastructure, Identification, Prioritization, and Protection," 17 December 2003, http://www.dhs.gov/homeland-security-presidential-directive-7.

[5] Ibid.

[6] *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington: DHS, 2009), 4, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[7] Ibid., 2.

[8] *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (Washington: DHS and DoD, May 2007), 3, http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

[9] *National Infrastructure Protection Plan*, 1–6, well summarizes the plan.

[10] *National Infrastructure Protection Plan*.

[11] *Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011), http://www.defense.gov/news/d20110714cyber.pdf.

[12] *NATO 2020: Assured Security; Dynamic Engagement—Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 11, 14, 20 (Brussels: NATO, 17 May 2010), http://www.nato.int/strategic-concept/expertsreport.pdf.

[13] Dan Auerbach and Lee Tien, "Dangerously Vague Cybersecurity Legislation Threatens Civil Liberties," *Electronic Frontier Foundation*, 20 March 2012, https://www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation.

[14] "Testimony of David Mahon, Vice President and Chief Security Officer, Century Links, Inc., before the Subcommittee on Communications and Internet Committee on Energy and Commerce, U.S. House of Representatives, March 7, 2012," 1, HHRG-112-IF16-Wstate-DMahon-20120307.pdf.

[15] John Hagel III, John Seely Brown, and Lang Division, *The Power of Pull* (New York: Basic Books, 2010), 31.

[16] William J. Lynn III, "Remarks on Cyber at RSA Conference," 15 February 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1535.

[17] The Russian Federation denies state complicity, although many suspect it acted through proxies.

18. James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February–March 2011): 23–40, http://www.iiss.org/publications/survival/survival-2011/year-2011-issue-1/stuxnet-and-the-future-of-cyber-war/.

19. Only 60 percent of Stuxnet infections affected Iranian facilities. Ibid.

20. See James Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy* 54, no. 12 (August–September 2012): 107–20.

21. Ibid.

22. Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, a report prepared for the US-China Economic and Security Review Commission (Washington: Northrop Grumman Corp., 7 March 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

23. Ibid., 13.

24. Sydney J. Freedberg Jr., "They're Here: Cyber Experts Warn Senate that Adversary is Already inside U.S. Networks," *AOL Defense*, 21 March 2012, http://defense.aol.com/2012/03/21/they-re-here-cyber-experts-warn-senate-that-adversary-is-alread/.

25. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no.5 (September/October 2010): 97–108, https://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain; and Sharon Weinberger, "Pentagon Official Says Flash Drive Used in Classified Attack," *AOL News*, 25 August 2010, http://www.aolnews.com/2010/08/25/pentagon-official-says-flash-drive-used-in-classified-cyberattac/. See also Kim Zetter, "The Return of the Worm that Ate the Pentagon," *Wired*, 9 December 2011, http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/.

26. "Operation Buckshot Yankee: Key Players and Networks Infected," *Washington Post*, 8 December 2011, http://www.washingtonpost.com/world/national-security/key-players-in-operation-buckshot-yankee/2011/12/08/gIQASJaSgO_story.html; and Zetter, "Return of the Worm."

27. David Alexander, "Pentagon Tries to Lean Forward in Cyberdefense," *Aviation Week*, 14 July 2011.

28. Lynn, "Defending a New Domain," 1.

29. Weinberger, "Pentagon Official Says Flash Drive Used."

30. Rob Rosenberger, "Gov't Hype Surrounds 'Operation Buckshot Yankee,' " *Vmyths*, 26 August 2010, http://vmyths.com/2010/08/26/oby/.

31. "Solar Sunrise," *GlobalSecurity.org*, 7 May 2011, http://www.globalsecurity.org/military/ops/solar-sunrise.htm.

32. Smith received a 20-month prison sentence and a $5,000 fine. Linda Rosencrance, "Melissa Virus Author Sentenced," *PC World*, 1 May 2002.

33. Ibid.

34. Michael Arrington, "Google Defends against Large Scale Chinese Cyber Attack: May Cease Chinese Operations," *Techcrunch.com*, 12 January 2010, http://techcrunch.com/2010/01/12/google-china-attacks/.

35. Robin Sidel, "Card Processor: Hackers Stole Account Numbers," *Wall Street Journal*, 1 April 2012, http://professional.wsj.com/article/SB10001424052702304750404577318083097652936.html?mod=WSJPRO_hpp_LEFTTopStories.

36. Michael Hickins, "The Morning Download: 'Prepare Yourself to be Penetrated,' " *CIO Journal*, 2 April 2012, http://blogs.wsj.com/cio/2012/04/02/the-morning-download-prepare-yourself-to-be-penetrated/?KEYWORDS=cybersecurity.

37. Devlin Barrett, "U.S. Outgunned in Hacker War," *Wall Street Journal*, 28 March 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html?KEYWORDS=cybersecurity.

38. Michael Balboni, "Halt, Who Hacks There?" *Newsday*, 27 January 2012.

39. Ibid.

40. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, 8 April 2009, http://online.wsj.com/article/SB123914805204099085.html. The article stated the intrusions were detected by US intelligence agencies, who said water, sewage, and other infrastructure systems were also at risk.

41. Ibid.

42. James Jay Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station: Texas A&M University Press, 2011), 9.

43. Jose Antonio Vargas, "The Face of Facebook," *New Yorker*, 20 September 2010, http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas.

44. Steve Bertoni, "Sean Parker: Agent of Disruption," *Forbes*, 21 September 2011, http://www.forbes.com/sites/stevenbertoni/2011/09/21/sean-parker-agent-of-disruption/4/.

45. Paul Festa and Joe Wilcox, "Experts Estimate Damages in the Billions for Bug," *CNET*, 5 May 2000, http://news.cnet.com/2100-1001-240112.html.

46. Eric Warner, "Global Cyber Supply Chain Management," *Microsoft Security Blog*, 26 July 2011, http://blogs.technet.com/b/security/archive/2011/07/26/global-cyber-supply-chain-management.aspx.

47. "Testimony of Dr. James Peery, Director of the Information Systems and Analysis Center, Sandia National Laboratories, Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 20 March 2012," 7.

48. Barrett, "U.S. Outgunned in Hacker War."

49. Jim Finkle and Andrea Shalal-Esa, "Exclusive: Hackers Breached U.S. Defense Contractors," *Reuters*, 27 May 2011, http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527; and Christopher Drew and John Markoff, "Lockheed Strengthens Network Security after Hacker Attack," *New York Times*, 29 May 2011, http://www.nytimes.com/2011/05/30/business/30hack.html.

50. Drew and Markoff, "Lockheed Strengthens Network Security."

51. Arthur W. Coviello Jr. (executive chairman, RSA), "Open Letter to RSA Customers," http://www.rsa.com/node.aspx?id=3872.

52. Jaikumar Vijayan, "Caution Urged in Wake of RSA Security Breach," *Computerworld*, 19 March 2011, http://www.computerworld.com/s/article/9214800/Caution_urged_in_wake_of_RSA_security_breach?taxonomyId=203&pageNumber=2.

53. Andrew Kemshall, "The RSA Security Breach—12 Months down the Technology Turnpike," *Huffington Post*, 14 March 2012, http://www.huffingtonpost.co.uk/andrew-kemshall/the-rsa-security-breach-1_b_1344643.html.

54. EMC Corporation SEC Form 8-K, dated 17 March 2011, http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/d8k.htm.

55. Hathaway, interview.

56. Siobhan Gorman, "Cybersecurity Bills Duel over Rules for Firms," *Wall Street Journal*, 9 March 2012, http://online.wsj.com/article/SB10001424052970203961204577269832774110556.html?KEYWORDS=cybersecurity.

57. Permanent Select Committee on Intelligence, "Committee Statement and Views," reporting on H.R. 3523, Cyber Intelligence Sharing and Protection Act, 5, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR3523CommitteeReport.pdf.

58. S 415, "Spectrum Optimization Act," 17 February 2011, http://www.gpo.gov/fdsys/pkg/BILLS-112s415is/pdf/BILLS-112s415is.pdf.

59. H.R. 4263, "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012," 27 March 2012, http://www.gpo.gov/fdsys/pkg/BILLS-112hr4263ih/pdf/BILLS-112hr4263ih.pdf. Representatives Mary Bono Mack and Marsha Blackburn introduced SECURE IT in the House.

60. S 415. For an excellent summary in layman's terms, see Stephen M. Spina and J. Daniel Skees, "Cybersecurity Act of 2012 Introduced," *National Law Review*, 21 February 2012, http://www.natlawreview.com/article/cybersecurity-act-2012-introduced.

61. Zach Walton, "Cybersecurity Act of 2012 Killed in the Senate," *WebProNews*, 2 August 2012, http://www.webpronews.com/cybersecurity-act-of-2012-killed-by-the-senate-2012-08; and The Revised Cybersecurity Act of 2012, S 3414, Summary: "This bill creates a 'public-private partnership' with private sector developed voluntary standards."

62. Mark M. Jaycox, "The Cybersecurity Act Was a Surveillance Bill in Disguise," *Guardian*, 2 August 2012, http://www.guardian.co.uk/commentisfree/2012/aug/02/cybersecurity-act-surveillance-bill-disguise; and Andrew Couts, "Senate Kills Cybersecurity Act of 2012," *Digital Trends*, 2 August 2012, http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/?utm_source=twitterfeed&utm_medium=twitter. The American Civil Liberties Union, however, supported the amended proposal because it included protections against passing private information to the National Security Agency or the military.

63. H.R. 3523, amending the National Security Act of 1947 (50 U.S.C. 442 et seq), http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523eh/pdf/BILLS-112hr3523eh.pdf.

64. The committee report on H.R. 3523 notes that while the bill does not define "private sector," it includes public, private, and quasi-public utilities that provide power, water, gas, and other critical services.

65. H.R. 3523, § 1104(b), pg. 6, line 11. The definitions sections of H.R. 3523 as passed are also subject to criticism as less than those contained in SECURE IT.

66. See Sherman Antitrust Act (Sherman Act), 15 U.S.C.A. 1-7, as amended by the Clayton Anti-Trust Act of 1914, 15 U.S.C. 12 et seq, notably § 1(a); the Federal Trade Commission Act of 1914, 15 U.S.C.A. 45 et seq, notably § 5 that applies to unfair methods of competition. The Sherman Act prohibits business activities that reduce competition in the marketplace and requires the federal government to investigate and pursue trust, companies, and organizations it suspects may violate the act. It makes illegal contracts, combinations in the form of trust or otherwise, or conspiracy in restraint of trade or commerce. The FTC Act authorizes the commission to enforce the antitrust laws.

67. 18 U.S.C. 2510, et seq; and 18 U.S.C. 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The Uniting and Strengthening America by Promoting Appropriate Tools Required to Intercept and Obstruct Terrorism—the USA PATRIOT Act, 18 U.S.C.A. 1 (Pub. L. 107-56, 107th Cong.) et seq, arguably weakened some provisions of the ECPA.

68. "Testimony of David Mahon," 2.

69. See Paul Rosenzweig, "Senate Cybersecurity Bill: Not Ready for Prime Time," *Heritage Foundation*, 7 March 2012, http://www.heritage.org/research/reports/2012/03/senate-cybersecurity-bill-not-ready-for-prime-time. Though critical of the proposed legislative, in his excellent assessment of Senator Joe Lieberman's bill, Rosenzweig agrees that provisions that enhance information sharing with other private-sector actors without fear of being prosecuted are a "solid improvement over current law." This author concurs with that view.

70. S 415, Title VII, § 701 et al.; H.R. 4263, Title 1, § 102; and H.R. 3523, § 1104 (b)(2).

71. S 415, § 702(b)(3); and H.R. 4263, §102.

72. The author conducted off-the-record interviews with attorneys who specialize in this challenge.

73. SECURE IT, § 102(g).

74. H.R. 3523, § 1104(b)(4), 9.

75. S 415, § 706.

76. Ibid.; H.R. 4263, § 102 (g); and H.R. 3523, § 701(b)(3).

77. 18 U.S.C. 2510, et seq; and 18 U.S.C. 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The Patriot Act arguably weakened some provisions of the ECPA.

78. S 415, § 707; H.R. 4263, § 102 (f); and H.R. 3523, § 701(e).

79. S 415, § 703(a); H.R. 4263, §§ 101 et al.; and H.R. 3523, § 1104(a).

80. H.R. 3523, § 704.

81. S 415, § 103(b)(2) and § 104(b)(2).

82. The problem is irrelevant to the other two bills, neither of which sets up a comprehensive regulatory scheme.

83. "Computer Security," *New York Times*, 27 April 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html.

84. See "Computer Security," *New York Times*, 14 March 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html; "Tracking Ghostnet," *Information Warfare Monitor*, 29 March 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-NetworkidUSL2E8EGGI320120316; "Shadows in the Cloud," *Information Warfare Monitor*, 6 April 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf; and Joseph Menn, "Microsoft Says Hacking Code Could Have Leaked," *Reuters*, 16 March 2012, http://www.reuters.com/article/2012/03/16/microsoftsecurity-commerce.senate.gov/public/?a=Files.Serve&File_id=e1244f6d-24ac-44b0-872e-61e1ce6509e6. See also Dian Bartz, "SECURE IT Act: Senate Republicans Introduce Softer Cybersecurity Bill," *Huffington Post*, 1 March 2012, http://www.huffingtonpost.com/2012/03/01/secure-it-act_n_1314213.html. SECURE IT would also reform federal cyber security standards.

85. S 415, Title I, § 103(a).

86. Text of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act of 2012, or SECURE IT.

87. See comments of Cong. Marsha Blackburn quoted in Amber Corrin, "House Republicans Issue Answer to Senate Cybersecurity Bills," *Federal Computer Week*, 1 March 2012, http://fcw.com/articles/2012/03/01/republican-cybersecurity-bill-secure-it-act.aspx.

88. Barrett, "U.S. Outgunned in Hacker War," remarks of Shawn Henry.

89. Ibid., 4.

90. "Testimony of Dr. Kaigham J. Gabriel, House Armed Service Committee, Subcommittee on Emerging Threats and Capabilities," 29 February 2012, 8.

91. Ibid., 7.

92. Ibid., 6.

93. "Statement of Dr. James N. Miller, Principal Deputy Undersecretary of Defense for Policy, U.S. Department of Defense, Hearing on National Defense Authorization Act for Fiscal Year 2012, Committee on Armed Services, U.S. House of Representatives," 16 March 2011, 4, http://www.fas.org/irp/congress/2011_hr/cybercom.pdf.

94. "What Keeps DARPA Leadership up at Night: Gabriel Testifies before House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities," DARPA news release, 29 February, 2012, http://www.darpa.mil/NewsEvents/Releases/2012/02/29a.aspx.

95. "Testimony of Dr. Kaigham J. Gabriel," 9.

96. "Testimony of Dr. James Peery."

97. See "Communications Security, Reliability and Interoperability Council III," *FCC Encyclopedia*, http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

98. See Domestic Security Alliance Council homepage, http://www.dsac.gov/Pages/index.aspx.

99. John Markoff, "Defying Experts, Rogue Computer Code Still Lurks," *New York Times*, 26 August 2009, http://www.nytimes.com/2009/08/27/technology/27compute.html?_r=1. It could be used to generate spam, steal passwords and logins, deliver fake antivirus warnings, and trick people into paying by credit card to have the infection removed. Ibid. See also Mark Bowden, *Worm* (Washington: Atlantic Monthly Press, 2011), which takes an in-depth look at the incident.

100. See Roger Hurwitz et al., "A Preliminary Report on the Cyber Norms Workshop," Center for Global Security Affairs, University of Toronto, 9, http://www.citizenlab.org/cybernorms/preliminary_report.pdf. This discussion of the Conficker challenge and how it was addressed is taken from their report.

101. Bowden, *Worm*, 231.

102. See "DNS Changer Malware," FBI, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf.

103. Melanie Hick, "DNS Changer Virus Spells 'Internet Doomsday,'" *Huffington Post UK*, 25 April 2012, http://www.huffingtonpost.co.uk/2012/04/25/dns-changer-virus-internet-doomsday_n_1451606.html.

104. See Jurgo-Soren Preden, "Enhancing Situation-Awareness, Cognition, and Reasoning of Ad-Hoc Network Agents" (PhD diss., Tallinn University of Technology, 2010), 46.

105. Jonathan Y. Huang and Margaret E. Kosal, "The Security Impact of the Neurosciences," *the bulletin.org*, http://www.thebulletin.org/web-edition/features/the-security-impact-of-the-neurosciences.

106. See Jonathan D. Moreno, *Mind Wars: Brain Research and National Defense* (New York: Dana Press, 2006), which focuses on the future in neuro-cyber weapons.

107. Preden, "Enhancing Situation-Awareness, 50.

108. See Preethi Vinayak Ponangi, "Cognitive Cyber Weapon Selection Tool Empirical Evaluation," Wright State University, 2007, 19.

109. See James Farwell, "PSYOP: A Tool for Administering Operational Shock in Cyber Space," *Perspectives* 22, nos. 1 and 2, (2012).

110. See, e.g., Hagel, Brown, and Division, *Power of Pull*, 134.

111. William J. Lynn, "Remarks on Cyber at the Council on Foreign Relations," 30 September 2010, http://www.defense.gov/speeches/speech.aspx?speechid=1509.

112. Ibid. Lynn also noted that collective defense with allies is a fourth strategy.

113. 18 U.S.C. 1030.

114. Richard Weitz, "Global Insights: The DHS' Cybersecurity Logjam," *World Politics Review*, 10 April 2012.

115. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009* (Washington: DHS, 2009).

116. Eric Chabrow, "Damn the Economy! IT Employment Rises to New Heights," *CIO Insight*, 1 July 2008, http://www.cioinsight.com/c/a/Trends/Damn-the-Economy-IT-Employment-Rises-to-New-Heights/.

117. "Testimony of Dr. James Peery," 8. Dr. Peery has asked Congress to support a Scholarship for Service Program that would strengthen the government's ability to recruit and retain top students.

118. Hathaway, interview.

119. See, e.g., "Committee Report on H.R. 3523, Permanent Select Committee on Intelligence," Report 112-445, 112th Cong., 2d sess., 8–9, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR3523CommitteeReport.pdf.

120. See, e.g., Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain (Wakefield, MA: SAFECode, 2010); *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain* (Wakefield: SAFECode, 2009); and Scott Charney and Eric T. Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," *Microsoft.com*, 25 July 2011, http://www.microsoft.com/en-us/download/details.aspx?id=26826.

121. Sandor Boyson, Thomas Corsi, and Hart Rossman, "Building a Cyber Supply Chain Assurance Reference Model," SAIC/Robert H. Smith School of Business, http://www.slamtheonlinescam.com/pdf/Cyber-Supply-Chain-Assurance.pdf.

122. See, e.g., Kathryn Stephens, "Cyber Supply Chain," NASCI white paper, 18 November 2010, http://www.nsci-va.org/WhitePapers/2010-11-18-Cyber%20Supply%20Chain%20Whitepaper-Stephens.pdf; Boyson, Corsi, and Rossman, "Building a Cyber Supply Chain"; Charney and Werner, "Cyber Supply Chain Risk Management"; and "Cyber Threats to National Security."

123. See Stephens, "Cyber Supply Chain."

124. Mark Crawford et al., *Defense Industrial Base Assessment: Counterfeit Electronics* (Washington: Department of Commerce, 2010), http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf. See also Stephens, "Cyber Supply Chain."

125. See Crawford et al., *Defense Industrial Base Assessment*.

126. "National Vulnerability Database Version 2.2," DHS/National Institute of Standards in Technology (NIST), http://nvd.nist.gov/.

127. Stephens, "Cyber Supply Chain." Her insightful analysis also recommends building a limited number of absolutely secure systems, creating a federal database of counterfeit products and suppliers, utilizing the General Services Administration to provide market incentives to provide security in hardware and software designs and the NIST to provide input. The NIST has recommended a risk management framework. See John Sankovich, "Cybersecurity: Continuous Monitoring Action Plan," *Information Week*, February 2011.

128. See, e.g., Wayne Rash, "Suppose IBM-Lenovo Deal Doesn't Happen," *eWeek.com*, 24 January 2005: http://www.eweek.com/c/a/Desktops-and-Notebooks/Suppose-IBMLenovo-Deal-Doesnt-Happen/.

129. See Michael Smith, "Spy chiefs fear Chinese cyber attack*,"* *Sunday Times*, 29 March 2009; Jeffrey Carr, "China's Silent Cyber Takeover?" *Diplomat*, 17 April 2011, http://the-diplomat.com/flashpoints-blog/2011/04/17/chinas-silent-cyber-takeover/; and John Tkacik Jr., "Trojan Dragon: China's Cyber Threat," Heritage Foundation backgrounder 2106, 8 February 2008, http://www.heritage.org/research/reports/2008/02/trojan-dragon-ch.inas-cyber-threat.

130. Dr. Ron Hart, interview by author.