Photo by Senior Airman Matthew Lancaster courtesy of the U.S. Air Force

Protecting the Nation's Critical Infrastructure from Cyber Attack

Lieutenant Colonel William A. Barnes
United States Marine Corps Reserve

Introduction

Imagine living in a world without cyberspace, unable to access email, cell phones, or social media. It is difficult to comprehend how much of our lives depend on information technology. The dependence goes well beyond our personal interactions with the plethora of emerging Internet-enabled gadgets and services. Cyberspace supports every

The opinions, conclusions, and recommendations expressed or implied within /luce.nt/ are those of the contributors and do not necessarily reflect the views of the Naval War College, the Department of the Navy, the Department of Defense or any other branch or agency of the U.S. Government.

aspect of our lives from energy to public transportation to healthcare. These essential services, along with others such as financial, water, and communications, collectively represent our critical infrastructure, as listed in Table 1. Recognizing the country's increasing reliance on technology and growing security threats in cyberspace, President George W. Bush issued "The National Strategy to Secure Cyberspace" in 2003. This strategy committed to defending the nation's critical infrastructure in order to protect the people, economy, and security of the United States.[1] Further, it highlighted the importance of a public-private partnership, describing this cooperative approach as the cornerstone for success.[2] Demonstrating an enduring commitment to this priority, President Barack Obama described cybersecurity among the country's most serious economic and security challenges, acknowledged the inadequacy of current defenses, and pledged to build upon efforts initiated by the prior administration.[3]

President Bush identified the Department of Homeland Security (DHS) as the federal center of excellence for cybersecurity.[4] President Obama further defined their responsibilities related to critical infrastructure security and resilience to include providing strategic guidance, promoting a national unity of effort, and coordinating the overall federal response.[5] These efforts established a cyberspace security response system, promoted awareness and training programs, and created forums for public-private information sharing. Unfortunately, progress to date does not adequately mitigate, deter, or prevent the most sophisticated cyber threats.[6] Since the nation's critical infrastructure remains susceptible to cyber attack, the U.S. Government must do more to accelerate the remediation of cyber vulnerabilities.

Table 1: Designated Critical Infrastructure Sectors[7]

Chemical	**Commercial Facilities**	**Communications**	**Critical Manufacturing**
Dams	**Defense Industrial Base**	**Emergency Services**	**Energy**
Financial Services	**Food and Agriculture**	**Government Facilities**	**Healthcare and Public Health**
Information Technology	**Nuclear Reactors, Materials, and Waste**	**Transportation Systems**	**Water and Wastewater Systems**

Background

Why is it so difficult to secure cyberspace? The answer is due in large part to the rate of technology development and associated complexity. The information revolution is actually an evolutionary process, where secure technologies eventually replace the insecure. Unfortunately, developing safe technologies is far from a trivial process. Gone are the days of simpler electronics such as the transistor radio where it was possible to conduct failure tests of every component to ensure proper function. Today's technology vendors consider security during product design and provide upgrades upon detecting vulnerabilities. The continued introduction of new technologies complicates the process by creating additional vulnerabilities and exposing those that did not previously exist. This trend of risk exposure continues to increase at an exponential rate.[8]

This increasing risk exposure encourages organizations intending harm. Our growing dependence on technology provides potential adversaries an opportunity to achieve increasing levels of disruption within our society. Within critical infrastructure, the potential is high enough to attract professional organizations representing nation states, criminal organizations, and extremist groups. Collectively, these actors develop highly sophisticated cyber exploits capable of circumventing current

defensive and detection capabilities. Gone are the days of the amateur "hacker" depicted in the movie *War Games*. Today's hackers are professionals with the backing of significant financial resources.[9]

In an effort to improve our response to emerging cyber vulnerabilities and exploitation, cybersecurity efforts prioritize public-private information sharing.[10] The premise is based on collective defense, where participants share new cyber threat information and implement appropriate prevention and detection measures. This information exchange provides technology vendors product feedback to prioritize future development efforts. In concept, this approach is both essential and reasonable. Unfortunately, various factors limit the effectiveness of these forums. The flow of information is predominately one-way, with the government providing the vast majority of contributions.[11]

Risk Exposure

In pursuit of increased performance and efficiency, organizations rely on emerging information technology capabilities and become more vulnerable to cyber exploitation. The level of vulnerability, or risk exposure, relates to the quantity of technology used. As a result of accelerating technology proliferation, risk increases at an exponential rate. As such, it is impossible to expect that testing alone can identify all potential vulnerabilities.

Unable to effectively anticipate vulnerabilities, the cybersecurity community accepts an enduring maintenance responsibility. Terms such as patch, signature, and firmware describe configuration changes that update technology products to the latest supported versions. For products such as a web browser, updates are relatively infrequent. For anti-virus software, updates occur more regularly, perhaps weekly or even daily. In some cases, technology exists to automate the upgrade process. In other cases, upgrades require significant manual intervention. Recognizing that unpatched systems are vulnerable to cyber threats, support teams attempt to complete upgrades as quickly as possible. Unfortunately, due to the vast number of upgrades released and the associated deployment complexity, many systems run without necessary upgrades for extended periods of time.[12] Within critical infrastructure, systems often run continuously in support of mission essential services. Under these circumstances, the only option is to defer the upgrade until a future scheduled maintenance period. Aside from long-term technology advancements that automate upgrade deployment and eliminate service outages, improvement in this area requires careful planning.

In addition to unpatched systems, significant risk exists within legacy technologies that persist well beyond their supported product life. We frequently upgrade smartphones with newer models, enjoying the benefits of faster performance, new features, and possibly improved security. Within critical infrastructure, some technologies operate for a decade or more, well beyond their supported product life. When a vendor terminates product support, commonly referred to as "end of life," it ceases developing patches to address new security vulnerabilities. This situation places those supporting such technologies in a difficult situation, as limited defensive options exist to address future vulnerabilities. This issue received considerable attention when Microsoft terminated support for the Windows XP operating system on April 8, 2014. Anticipating significant impact throughout the critical infrastructure environment, the ICS-CERT issued a notification in May 2012 reminding the entire community of the deadline to complete necessary upgrades. In this message, ICS-CERT acknowledged industrial control vendors and integrators resistance to supporting new operating systems because of compatibility concerns.[13] As a result, in many cases upgrade options did not exist. Organizations had to choose between replacing current technology with a new product and operating at risk.

Within our society, various mechanisms exist to address situations of abandonment. In the case of an abandoned child, protective services organizations intervene. In the case of an abandoned home, a local government takes possession or a mortgage company conducts foreclosure. No such parallel exists in cyberspace. Technology vendors can terminate support of any product at a time of their choosing, leaving a community of existing users in a difficult situation. While companies have every right to decide how to support their products, consumers of these products deserve protection from the consequences of abandoned products.[14] This is an area where the U.S. Government must take action to provide technology consumers an option to defend themselves.

Threat Sophistication

Beyond the struggles of deploying necessary security updates to critical infrastructure, we must recognize the growing exposure associated with the proliferation of new automation capabilities. As with our personal lives, digitally connected in ways considered impossible just a few years ago, critical infrastructure becomes more integrated with emerging automation. Driven by the benefits of performance, efficiency, and cost, this integration also creates an increasingly valuable target for those attempting to disrupt the society, economy, and security of the United States. To seize upon this opportunity, foreign governments, extremist groups, and criminal organizations dedicate tremendous resources to develop sophisticated cyber weapons that exploit unknown vulnerabilities.

Upon disclosure of a weakness, the cybersecurity community can develop a defensive capability. Until then, those with knowledge of the vulnerability possess supreme power, able to develop exploits and conduct attacks without concern of detection. The cyber equivalent of invisibility, the term "zero-day" describes vulnerabilities unknown to the public.[15] In the past, governments maintained a zero-day monopoly.[16] The situation today is much different.

In 2005, as the Department of Defense expanded efforts related to cyber warfare, many companies emerged offering offensive cyber capabilities.[17] Beyond traditional defense contractors such as Northrup Grumman, Raytheon, and General Dynamics, many specialized companies emerged offering unique cyber weapons, including some designed specifically for critical infrastructure.[18] Participants in this new and lucrative market include Vupen (Montpellier, France); Netragard (Acton, MA); Exodus Intelligence (Austin, TX); Endgame (Virginia); and ReVuln (Malta).[19] Not surprisingly, these vendors do not disclose the identity of their clients but acknowledge that some of the largest customers are government agencies.[20] Internationally, the largest investors include Israel, Britain, Russia, India and Brazil. Additionally, North Korea, Malaysia, Singapore, and many Middle Eastern intelligence services purchase information related to computer vulnerabilities.[21]

The creation of the cyber vulnerability industry institutionalized the amateur hacker. With more easily identified vulnerabilities resolved by a maturing industry, only the most gifted amateurs exhibit the skills necessary to detect new security flaws. Lacking the financial means to perform adequate testing to prevent detection, they depend upon support from the larger profession.[22] The current CryptoLocker virus illustrates the increasing level of sophistication. When CryptoLocker infects a computer, the virus encrypts all of the data, denying the user access to files and data. CryptoLocker allows the user to remove the encryption if they pay a fee through an untraceable electronic method. Having experienced the cyber equivalent of a perfect crime, the police department in Swansea, Massachusetts, recently paid a $750 ransom to restore important computer files.[23]

Currently, many zero-day vendors can supply more than one hundred exploits per year at an approximate cost of $40,000 to $160,000 each.[24] Vupen claims they do not sell to any country subject to

embargo or trade restriction by the European Union, United States, or United Nation. Vupen customers pay a $100,000 subscription fee in order to view the catalogue of available exploits, which they must purchase separately.[25] Providing services strictly to U.S. customers, Netragard's exploit acquisition program doubled in the last three years, with rates for security flaws ranging between $35,000 and $160,000.[26] A former director of the National Security Agency (NSA) supports the start-up Endgame, which sells vulnerability information primarily to the U.S. Government.[27] Revuln specializes in critical infrastructure targeting industrial control systems.[28]

iDefense created the Vulnerability Contributor Program (VCP) in 2002. Three years later Tipping Point launched the Zero Day Initiative (ZDI).[29] The purpose of both programs is to purchase vulnerability information before public disclosure, permitting vendors an opportunity to resolve the problem.[30] With the intent of improving the safety of cyberspace, both programs established ethical standards. Unable to resell vulnerabilities to the highest bidder, these programs cannot pay contributors a prevailing market rate.[31] As a result, it seems likely that vulnerabilities reported through these purchase programs represent just the tip of the iceberg. Even so, their results demonstrate the magnitude of the problem. As of September 2013, VPC and ZDI collectively have purchased 2,393 vulnerabilities since their inception.[32] The average duration from vulnerability purchase to public disclosure is 133 days for VCP and 174 days for ZDI.[33] A 2012 study by Symantec Research Labs found that zero-day exploits exist for an average of 312 days and as long as thirty months before public disclosure.[34] This study also found that after public disclosure the volume of related attacks increased by up to five orders of magnitude.[35] Vulnerability periods ranging between 113 days and thirty months provide a lot of time for those seeking to take advantage of the situation. Vendors with the most vulnerabilities identified through the VCP and ZDI programs include Microsoft, Apple, HP, Adobe, and Oracle.[36] These vendors' products include the operating systems, databases, office automation software, and management utilities that run on nearly every computer and a large percentage of industrial control systems.

To address the issue of zero-day vulnerabilities, some vendors established "bug bounty programs" to purchase information prior to public disclosure or sale on the black market.[37] Over a three year period, Google paid $580,000 for 501 vulnerabilities in the Chrome web browser.[38] During the same time, Mozilla paid $570,000 for 190 vulnerabilities in its competing web browser, Firefox.[39] Facebook paid approximately $1,000,000 since creating its program in 2011.[40] In June 2013, Microsoft, after years of resisting such an approach, established a formal program, paying approximately $100,000 to date.[41] The recent growth of these programs suggests the approach represents the best option for quickly and discretely addressing vulnerabilities.

Information Sharing

Recognizing the significance of growing risk exposure and increasingly sophisticated attacks, the earliest efforts to secure cyberspace stressed the importance of developing a public-private partnership. President Bush stated that in order to build a more secure future in cyberspace, public and private organizations must act together.[42] The importance of developing robust information sharing capabilities endures as a fundamental priority for President Obama's administration.[43,44] This commitment led to the creation of numerous information sharing forums, including the Information Sharing and Analysis Centers (ISACs), the U.S. Computer Emergency Response Team (US-CERT), and the National Cybersecurity and Communication Integration Center (NCCIC).[45] Fifteen ISACs currently exist, representing the various critical infrastructure sectors. They include financial services (FS-ISAC), national health (NH-ISAC), and water (WaterISAC).[46] In addition to these information sharing forums, the Federal Bureau of Investigation (FBI) established InfraGard, which brings together representatives from business, academia, state and local law enforcement agencies, and other interested parties to prevent

hostile acts against the United States.[47] In recent years, additional non-profit entities emerged, such as the Advanced Cyber Security Center (ACSC), which promotes cybersecurity research and development, education, and thought leadership throughout New England.[48] Those seeking to engage in dialogue related to cybersecurity have many options.

Although sufficient quantity exists, the quality of information sharing falls well below the intended goal. Information exchanged with DHS and other government agencies frequently is outdated or too generic in nature for use by participating members. In other cases, information shared by DHS is over-classified, preventing disclosure to the private sector. Efforts to place members of the information technology ISAC (IT-ISAC) on the floor of the NCCIC failed due to various legal issues.[49] Despite these challenges, private industry continues to seek government assistance upon detecting a compromise. For example, more than 40 percent of those supporting SCADA systems acknowledge reporting issues to an appropriate government agency.[50] While this represents an essential step in the right direction, changes are necessary to eliminate remaining barriers to information sharing.

In an effort to address information sharing challenges, specifically security classification, DHS established the Enhanced Cybersecurity Services (ECS). The purpose of ECS is to expand the number of companies that receive classified information related to real or potential threats.[51] This program emerged following a successful pilot known as the Defense Industrial Base (DIB) Pilot, which enabled classified information sharing with several internet service providers.[52] Although more than fifty companies initially expressed interest in ECS, not one joined the program.[53] The cost associated with building a classified network and legal issues rank among the most significant roadblocks impacting enrollment.[54] DHS notes much better progress with unclassified programs, although the sharing of information is predominately one-way, initiated by the government.[55]

Despite presidential recognition that the future of cybersecurity depends upon public-private information sharing, many bureaucratic challenges remain that impede progress. Organizations resist sharing threat information in order to protect their reputation. Unless convinced that disclosures are anonymous, this hesitation will continue. Consider public health, where the issue of privacy is paramount. That is until a patient seeks medical attention for rare and dangerous illnesses. In such cases, reporting is mandatory, and public safety supersedes patient privacy.[56] Cybersecurity needs a similar process to report the most dangerous threats. Seeking to promote continued information sharing, the United States must realize that continuing disclosures by Edward Snowden cast doubt in the minds of Americans regarding the government's true intention regarding cybersecurity. Similar to recently announced changes to National Security Agency (NSA) surveillance policies, establishing a panel of advocates on information sharing challenges could solve many of the security classification concerns and related bureaucratic obstacles.[57] The solution to the security of our critical infrastructure is collective defense. We must improve our ability to tap into the experience and knowledge of all interested parties.

Conclusion

Our society and economy rely on the nation's critical infrastructure. Recognizing the importance of these essential services and the growing threat of cyber attack, two presidential administrations prioritized efforts to secure cyberspace. The resulting government led initiatives captured the attention of industry, media, and the world. Despite recognition and significant effort, cybersecurity remains an elusive goal. The primary reasons for the lack of progress related to critical infrastructure are the growing risk associated with the proliferation of automation technologies, increasingly sophisticated cyber threats, and an inability to establish effective public-private information sharing.

On a daily basis, the media reminds the world of the clear and present dangers of cybersecurity. Stuxnet and CryptoLocker demonstrate that determined organizations, whether a state or criminal organization, can harness vulnerabilities within cyberspace to their advantage. The battle between exploiting and mitigating vulnerabilities in cyberspace created the cyber equivalent of an arms race. Despite continued risks, a more secure cyberspace is possible. Cyberspace is the creation of mankind, and we possess the ability to create a more secure future by harnessing the lessons from past oversight and omission. An evolutionary process, this will take vigilance, time, and continual assessment.

Recommendations

While a more secure cyberspace will emerge through an evolutionary process, with immediate action the U.S. Government can influence the rate of change. By executing the recommendations described below, the nation can simultaneously address the increasing risk exposure, growing threat sophistication, and impediments to information sharing.

Risk Exposure

The U.S. Government must act to reduce the impact of vendors abandoning product support. Specifically, the Department of Commerce must require vendors who terminate support for an information technology product to share the source code with DHS. Additionally, DHS must securely store the source code and grant access to authorized representatives of the user community, thereby providing an opportunity to resolve or mitigate future security vulnerabilities.

Threat Sophistication

The U.S. Government must provide financial incentives to promote programs that accelerate the identification and remediation of zero-day vulnerabilities. Specifically, DHS and DOD must jointly define the highest priority risks and provide funding to establish a government sponsored vulnerability purchase program. Additionally, DHS must develop mechanisms to encourage vendors to respond to disclosed vulnerabilities in a timely manner. One option involves creating a cybersecurity scorecard for information technology vendors. Vendors with fewer vulnerabilities and a more rapid response would receive higher ratings. Those responsible for purchasing information technology solutions within critical infrastructure industries could use these ratings to avoid less secure products.

Information Sharing

The U.S. Government must review current security classification standards related to cybersecurity and prioritize disclosure to those who can mitigate issues and those vulnerable to exploitation. Specifically, DHS must develop updated classification guidelines to maximize the ability to share information within the critical infrastructure community. DHS must also engage the DOD to ensure the consistent application of revised classification guidelines. Additionally, DHS must establish mandatory cybersecurity reporting guidelines. To ensure maximum compliance, the process must permit anonymous reporting. Finally, DHS must provide timely updates to the critical infrastructure community regarding reported incidents along with detection and response recommendations.

---

1. The White House, "The National Strategy to Secure Cyberspace," *The White House - President George W. Bush,* (2003), 4, http://georgewbush-whitehouse.archives.gov/pcipb/ (accessed January 14, 2014).
2. Ibid., 4.

3. President of the United States, "Foreign Policy," (May 2009), 1, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed January 14, 2013)
4. The White House, "The National Strategy to Secure Cyberspace," *The White House - President George W. Bush*, (2003), 10, http://georgewbush-whitehouse.archives.gov/pcipb/ (accessed January 14, 2014)
5. The President of the United States, "Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience," (February 12, 2013), 2, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 14, 2014).
6. Dan Geer, interview by William Barnes, CISO at *In-Q-Tel* (January 10, 2014)
7. The President of the United States, "Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience," (February 12, 2013), 2, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 14, 2014)
8. Dan Geer, interview by William Barnes, CISO at *In-Q-Tel* (January 10, 2014).
9. Ibid.
10. President of the United States, "Executive Order - Improving Critical Infrastructure Cybersecurity," (February 12, 2013), 1, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed January 14, 2014).
11. Jason Miller, "DHS Finds Classified Cyber Sharing Program Slow to Take Off," *Federal News Radio*, (June 13, 2013), http://www.federalnewsradio.com/473/3356694/DHS-finds-classified-cyber-sharing-program-slow-to-take-off (accessed January 14, 2014).
12. The White House, "The National Strategy to Secure Cyberspace," *The White House - President George W. Bush*, (2003), 33, http://georgewbush-whitehouse.archives.gov/pcipb/ (accessed January 14, 2014).
13. ICS-CERT, *ICS-CERT Monthy Monitor*, (May 2012), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May2012.pdf (accessed January 16, 2014)
14. Dan Geer, interview by William Barnes, CISO at *In-Q-Tel* (January 10, 2014).
15. Stefan Frei, "NSS Labs" *The Known Unknowns*, (December 2013), 16, https://www.nsslabs.com/system/files/public- report/files/The%20Known%20Unknowns_0.pdf (accessed January 14, 2014)
16. Ibid., 1.
17. Michael Riley and Ashlee Vance, "Bloomberg Business Week," *Cyber Weapons: The New Arms Race*, (July 20, 2011), 2, http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p1 (accessed January 19, 2014)
18. Ibid.
19. Nicole Perlroth and David E. Sanger, "The New York Times," *Nations Buying as Hackers Sell Flaws in Computer Code*, (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=0 (accessed January 19, 2014).
20. Stefan Frei, "NSS Labs" *The Known Unknowns*, (December 2013), 13, https://www.nsslabs.com/system/files/public-report/files/The%20Known%20Unknowns_0.pdf (accessed January 14, 2014)
21. Nicole Perlroth and David E. Sanger, "The New York Times," *Nations Buying as Hackers Sell Flaws in Computer Code*, (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=0 (accessed January 19, 2014)
22. Dan Geer, interview by William Barnes, CISO at *In-Q-Tel* (January 10, 2014)
23. Melissa Hanson, *The Boston Globle - Swansea Police Department pays ransom to computer hackers*, (November 19, 2013), http://www.bostonglobe.com/metro/2013/11/19/swansea-police-pay-ransom-open-files-locked-hackers/7bOdi8i7foNkTmdnokMAkP/story.html (accessed January 16, 2014)
24. Stefan Frei, "NSS Labs" *The Known Unknowns*, (December 2013), 14, https://www.nsslabs.com/system/files/public-report/files/The%20Known%20Unknowns_0.pdf (accessed January 14, 2014).

25. Nicole Perlroth and David E. Sanger, "The New York Times," *Nations Buying as Hackers Sell Flaws in Computer Code*, (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=0 (accessed January 19, 2014)
26. Ibid.
27. Ibid.
28. Ibid.
29. Stefan Frei, "NSS Labs" *The Known Unknowns*, (December 2013), 8, https://www.nsslabs.com/system/files/public- report/files/The%20Known%20Unknowns_0.pdf (accessed January 14, 2014).
30. Ibid.
31.Ibid.
32. Ibid.
33. Ibid., 9
34. Leyla Bilge and Tudor Dumitras, "Before We Knew It - An Emperical Study of Zero-Day Attacks in the Real World," *19th ACM Conference on Computer and Communications Security*, Raleigh, NC, (2012), 11.
35. Ibid.
36. Stefan Frei, "NSS Labs" *The Known Unknowns*, (December 2013), 10, https://www.nsslabs.com/system/files/public- report/files/The%20Known%20Unknowns_0.pdf (accessed January 14, 2014).
37. Ibid., 13
38. Ibid., 13
39. Ibid., 13
40. Ibid., 13.
41. Ibid., 13
42. The White House, "The National Strategy to Secure Cyberspace," *The White House - President George W. Bush*, (2003), 4, http://georgewbush-whitehouse.archives.gov/pcipb/ (accessed January 14, 2014).
43. The President of the United States, "Foreign Policy," (May 2009), 5, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed January 14, 2013).
44. The President of the United States, "Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience," (February 12, 2013), 1, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 14, 2014)
45. Information Technology Industrial Council, *ITI Recommendation: Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity*, (October 2011), 2, http://www.itic.org/dotAsset/8be757cb-88e8-48ce-86a9-0d365db9d016.pdf (accessed January 14, 2014)
46. National Council of ISACs*, Member ISACs*, (no date), http://www.isaccouncil.org/memberisacs.html (accessed January 19, 2014).
47. InfraGard, *Partnership for Protection*, (no date), https://www.infragard.org/ (accessed January 19, 2014).
48. Advanced Cyber Security Center, *About Us*, (no date), http://www.acscenter.org/about/ (accessed January 19, 2014).
49. Information Technology Industrial Council, *ITI Recommendation: Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity*, (October 2011), 4-5, http://www.itic.org/dotAsset/8be757cb-88e8-48ce-86a9-0d365db9d016.pdf (accessed January 14, 2014)
50. Luallen, Matthew E, *SANS SCADA and Process Control Security Survey*, (February 2013), 15, https://www.sans.org/reading-room/analysts-program/sans-survey-scada-2013 (accessed January 14, 2014)
51. Jason Miller, "DHS Finds Classified Cyber Sharing Program Slow to Take Off," *Federal News Radio*, (June 13, 2013), http://www.federalnewsradio.com/473/3356694/DHS-finds-classified-cyber-sharing-program-slow-to-take-off (accessed January 14, 2014).
52. Ibid.
53. Ibid.
54. Ibid.

55. Ibid.
56. Dan Geer, interview by William Barnes. CISO at *In-Q-Tel* (January 10, 2014).
57. Mark Landler and Charlie Savage, "The New York Times," *Obama Outlines Calibrated Curbs on Phone Spying*, (January 17, 2014), http://www.nytimes.com/2014/01/18/us/politics/obama-nsa.html (accessed January 20, 2014).