International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: http://www.tandfonline.com/loi/ujic20

U.S. Cyber Threat Intelligence Sharing Frameworks

Scott E. Jasper

To cite this article: Scott E. Jasper (2017) U.S. Cyber Threat Intelligence Sharing Frameworks, International Journal of Intelligence and CounterIntelligence, 30:1, 53-65, DOI: 10.1080/08850607.2016.1230701

To link to this article: http://dx.doi.org/10.1080/08850607.2016.1230701

Published online: 02 Nov 2016.

International Journal of Intelligence and CounterIntelligence, 30: 53–65, 2017
Copyright © Taylor & Francis Group, LLC
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2016.1230701

SCOTT E. JASPER

U.S. Cyber Threat Intelligence Sharing Frameworks

Malicious actors in cyberspace are gaining increasingly sophisticated tools, techniques, and procedures that are outpacing security solutions. Organized criminals and state-sponsored groups now have ample resources to disrupt or breach conventional defenses. Underground hacker markets provide them with ready access to a plethora of products and services.[1] Attackers often rent large botnets or use similar attack tool kits. For instance, the intelligence firm Crowdstrike recently found twelve malicious groups in China using the same exploit codes within 24 to 72 hours of each other.[2] In many cases, malicious attempts to obtain valuable, sensitive data are not isolated, but part of multi-year campaigns. For their victims, the costs of a successful attack can add up in professional services, lost opportunities, and downtime, plus reputation damage, to almost a million dollars.[3] Targeted

Captain Scott E. Jasper, a retired United States Navy officer, is a faculty member in the National Security Affairs Department at the Naval Postgraduate School, Monterey, California. He was previously Associate Dean of the School's International Graduate Studies program. An alumnus of the U.S. Naval Academy, Annapolis, Maryland, he earned a Master's degree in Business Administration at San Jose State University, a Master's degree in National Security and Strategic Studies from the Naval War College, Newport, Rhode Island, and is currently a doctoral candidate in Politics at the University of Reading in the United Kingdom. In the Navy, he served as Deputy for Joint Experimentation at the headquarters of the U.S. Pacific Command. Captain Jasper is the editor of Conflict and Cooperation in the Global Commons *(Washington, DC: Georgetown University Press, 2012) and* Securing Freedom in the Global Commons *(Stanford, CA: Stanford University Press, 2010).*

organizations need a holistic view of the threat landscape and a proactive security posture to defend against the multitude of threats. Knowing the who, what, where, how, and when of a malicious activity is the only way to decrease its chance of success. Cyber threat intelligence provides knowledge of a malicious actor's capabilities, infrastructure, motives, goals, and resources in cyberspace. The use of this intelligence enables an organization to prioritize defenses around prized assets, focusing on vulnerabilities and ways that an adversary activity can be mitigated.[4]

Cyber attacks may be part of coordinated campaigns that simultaneously target related organizations by sector, whether industry or commercial. Based on actual attacks observed during 2014 by the cyber security company Risk Analytics, 75 percent of attacks spread from Victim 0 to Victim 1 within one day, while over 40 percent hit the second organization in less than an hour. A sense of urgency exists to share what is known about attacks, because the faster and more broadly various types of cyber threat intelligence are shared, the more other organizations can theoretically stop similar attacks.[5] Recipient organizations can leverage cyber threat intelligence in the form of cyber threat information and indicators across various cyber attack vectors in support of improved data analytics and layered security controls. Cyber threat intelligence allows an organization to stay ahead of a malicious actor. The visibility it provides lets an affected organization understand the tradecraft of sophisticated attackers and make informed decisions to better protect from targeted assaults.

CYBER THREAT INTELLIGENCE CONFIGURATIONS

Threat intelligence is formed through information gathered from disparate sources synthesized by human analysts to identify a specific threat to a specific target. The discipline of intelligence fuses any combination of human intelligence (HUMINT)—the collection of information from human sources; open source intelligence (OSINT)—the exploitation of public information via data mining; signals intelligence (SIGINT)—the collection of signals transmitted by communications systems; imagery intelligence (IMINT)—the use of images from terrestrial, airborne, or satellite collectors; and measurement and signature intelligence (MASINT)—the use of information gathered by technical instruments.[6] Cyber threat intelligence applies broader principles of intelligence which include the collection of information from many sources, context-aware analysis, intelligence production, and delivery to consumers. The intelligence cycle consists of planning and direction for intelligence gathering; the collection of potentially useful raw data from relevant sources; the processing of collected data into a standardized format for detailed analysis; the analysis of processed data to identify threats to customers and suitable countermeasures; and the dissemination of the analysis in the context of cyber threat information and indicators to consumers so that appropriate protective measures can be taken.[7]

The idea behind cyber threat intelligence is to provide the ability to recognize and act upon relevant threats in a timely manner. Effective cyber threat intelligence exhibits the characteristics of being actionable. That means it should ideally identify actions the recipient can take to counter a threat or provide an adequate context to develop a suitable response. To counter a fast moving cyber assault, the intelligence products should be delivered within minutes or seconds. In dealing with a more deliberate attack, the intelligence may still be useful if hours, days, or even months old. Whenever and however it arrives, cyber threat intelligence should be relevant to an organization. It should address threats the organization is likely to face, attacks it is likely to experience, and describe the malicious elements the recipient is likely to encounter. Intelligence should be accurate, meaning correct, complete, and unambiguous.[8] Cyber threat intelligence is constructed and delivered in the context of cyber threat information or indicators. Among its many forms are annual or quarterly threat reports (such as in PDF or Word documents), vendor blogs, email alerts, and data feeds by structured file formats. Overall, cyber threat intelligence products should be demonstrably useful to the defense of organizational assets. For example, threat indicators that increase detection capability and provide early warning of attack are of the most immediate value.

Threat indicators can be classified as either indicators of compromise or indicators of attack. Indicators of compromise are typically the presence of malware, signatures, exploits, vulnerabilities, and Internet Protocol (IP) addresses. Indicators of attack may signal that an attack is underway, such as in code execution, persistence, stealth, command and control, and lateral movement within a network. A combination of indicator of attack analysis with indicator of compromise protection can address the full range of attacks.[9] Organizations rely on multiple data feeds for aggregation and analysis. They accept and consolidate technical data through their security information and event management (SIEM) and intrusion prevention system (IPS) platforms. This data consists of specific attacker attributes and granular indicators, like malware samples or vulnerability information. Other examples of useful data are command and control channels or destination IP addresses. Cyber threat intelligence products help defenders detect attacks during, and ideally before, stages of an attack, by providing indicators of actions taken during every stage. For instance, security alerts and logs provide visibility on access creation, configuration modifications, and database events, while other reported indicators include remote logins from atypical countries, access outside of hours, and changes to privileged accounts.[10] With sound data, security teams can more readily look for indicators and patterns of malicious activity.

Intelligence Sources

An organization can leverage cyber threat intelligence from internal, commercial, or community sources. Internally, organizations collect and develop intelligence from resident capabilities. In some cases, an organization can find signs that an attack may occur in the future, for example, through Web server log entries that show the usage of a vulnerability scanner. More common is the detection of indicators of attack, like a network intrusion detection sensor that alerts when a buffer overflow attack attempt occurs against a database server, or of compromise, like antivirus software that alerts when it detects that a host is infected with malware. Other internal indicators are file integrity checking software, network flow sensors, and operating system, service, and application logs, which record which accounts were accessed and what actions were performed. Similar in function are network device logs from firewalls and routers which log blocked connection attempts.[11] The challenge is sorting and internally sifting through thousands or even millions of indicators a day to find the real security incidents that have occurred. This process is time-consuming, labor-intensive, and potentially error-prone.

Organizations can turn to commercial sources for cyber threat intelligence to reduce processing time and cut labor costs. They can find free cyber threat intelligence services on Internet-accessible outlets that distribute indicators of compromise, malware, and blacklist information. For example, Google's VirusTotal is a free online service that analyzes suspicious files and URLs (Web addresses like http://www.example.com/) to facilitate the quick detection of viruses, worms, Trojans, and all kinds of malware. VirusTotal also runs a blog site for the latest information on malware execution and URL parameters.[12] Likewise, some leading cyber security firms freely release news and analysis on their blogs, among them Unit 42 at Palo Alto Networks.[13] Still, information from open sources has to be manually collected and analyzed, so many organizations choose to obtain fused cyber threat intelligence from a commercial provider. A wide range of providers is available from which to choose. Many vendors supply data to support their technologies, and others provide data that is interoperable with corporate systems.[14] For instance, McAfee supplies cloud-based real-time global threat intelligence for McAfee products at no charge.[15] Likewise, Palo Alto Networks' cloud-based malware analysis WildFire environment offers protection from unknown threats (malware, exploits, command and control) through native integration with their Enterprise Security Platform.[16] In turn, LookingGlass provides multi-source, Internet-intelligence-based Virus Tracker data feeds that connect to corporate security infrastructure with an easy-to-use API (Application Program Interface).[17]

Organizations can also obtain cyber threat intelligence from a sharing community structured around such industry sectors as financial, electricity, or health. One type of sharing community arrangement is the Information Sharing and Analysis Center (ISAC). The concept of an ISAC was introduced and promulgated pursuant to Presidential Decision Directive-63 (PPD-63), signed by President Bill Clinton on 22 May 1998. PPD-63 directed the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism to consult with critical infrastructure owners and operators to encourage the creation of a private sector Information Sharing and Analysis Center. The Center could serve as a mechanism to not only gather, analyze, sanitize, and disseminate private sector information to both industry and the government, but also to distribute to the private sector government-produced threat information. Critical to the success of such an institution is its timeliness, accessibility, coordination, flexibility, utility, and acceptability.[18] Today, twenty ISACs exist to analyze and share timely, relevant, and actionable cyber security information as it pertains to threats, vulnerabilities, and incidents. ISACs also share security-best practices and empower resiliency through security planning and disaster response. Most ISACs have 24/7 threat warning and incident reporting capabilities.[19] ISACs reach deep into their sectors to provide trusted and secure information and analytical capabilities to communities, as they relate to aviation, communications, maritime, oil and natural gas, real estate, retail, transportation, and water.[20]

Another type of sharing community arrangement is the Information Sharing and Analysis Organization (ISAO). At his Cybersecurity Summit at Stanford University in February 2015, President Barack Obama signed a new Executive Order to encourage companies and industries to set up ISAOs to share threat information with each other. The Order promotes information sharing about cyber threats, both within the private sector and between government and the private sector.[21] ISAOs may be organized on the basis of sector, region, or other affinity, with membership drawn from the public or private sectors, or a combination of both. The Order calls for a common set of voluntary standards for baseline capabilities that ISAOs should possess. The standards address operating procedures, technical means, and privacy protections, such as minimization.[22] The National Council of ISACs is working collaboratively with its partners in implementing the Executive Order, although whether the new standards will apply to sector ISACs is not clear. Nonetheless, the National Council of ISACs remains engaged in many key industry segments that have been experiencing cyber attacks, often working with the National Cybersecurity and Communications Integration Center (NCCIC) during incidents.[23] The new Order also directs the NCCIC to engage in continuous coordination with the ISAOs on the sharing of information related to cybersecurity risks and incidents.

FEDERAL GOVERNMENT STRUCTURES

The Department of Homeland Security (DHS) is responsible for protecting U.S. critical infrastructure from physical and cyber threats. Inside the DHS resides the National Cybersecurity and Communications Integration Center (NCCIC), which serves as a central location where a diverse set of partners involved in cyber security coordinate and synchronize their efforts. Thirteen federal departments and agencies and sixteen private sector entities have regular, dedicated liaisons at the Center, while over 100 private sector entities collaborate with the Center on a routine basis. The NCCIC analyzes cyber security information, shares timely and actionable threat information, and coordinates response, mitigation, and recovery efforts.[24] Its Operations and Integration Branch plans, coordinates, and integrates capabilities to synchronize analysis, information sharing, and incident management efforts. The U.S. Computer Emergency Readiness Team is the NCCIC's 24-hour operational arm. The Team distributes vulnerability and threat information through its National Cyber Awareness System, which offers mailing lists for alerts on issues, bulletins on vulnerabilities, tips for the general public, and current security activity.

The National Cybersecurity and Communications Integration Center will partner with the new Cyber Threat Intelligence Integration Center (CTIIC) to protect national networks. This center will help the Department of Homeland Security better understand various cyber threats by providing targeted Intelligence Community support.[25] President Obama directed the Director of National Intelligence in February 2015 to establish the CTIIC. The purpose of the Center is to provide integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests. The CTIIC will not directly engage with the country's private sector entities to provide, receive, or obtain any information about cyber threats; instead, it will support the NCCIC in its mission.[26] Modeled after the National Counter-terrorism Center, the CTTIC will not collect intelligence, but will analyze and integrate information already collected under existing authorities to fill gaps between existing agencies.[27] However, even with significant responsibilities, the Center will not be allowed to fill more than 50 permanent positions, though it will be located in a building owned or operated by an element of the Intelligence Community.[28]

Voluntary Programs

The Department of Homeland Security conducts a variety of voluntary information sharing programs. The Cyber Information Sharing and Collaboration Program (CISCP) establishes a community of trust between the federal government and entities from critical infrastructure sectors. The program shares cyber threat, incident, and vulnerability information in near-real time, and enhances collaboration to improve network defense for the entire community. To join CISCP, partners such as the Information Sharing and Analysis Centers and the stakeholder community, sign a Cooperative Research and Development Agreement, which provides access to the NCCIC Watch Floor and clearances up to the TS/SCI level. CISCP participants submit threat indicators to the Department of Homeland Security, which can be shared with other participants in an anonymized, aggregated fashion. Upon receiving a submission, program analysts redact any personal or proprietary information and analyze the submission in collaboration with both government and industry. Any provided data classified as Protected Critical Infrastructure Information is protected by statute, exempting it from both release and regulatory use. Program analysts produce accurate, relevant, timely, and actionable analytical products that take the form of Indicator, Analysis, and Alert Bulletins and of Recommended Best Practices.[29]

Another voluntary information sharing program run by the Department of Homeland Security is the Enhanced Cybersecurity Services (ECS) program. This program is an enhanced approach to protect and defend U.S. based public and private entities by supplementing commercial services and capabilities with government threat information. The ECS program shares sensitive and classified government-vetted cyber threat information with qualified and cleared private sector cyber security Commercial Service Providers (CSPs) and also Operational Implementers (OIs). The CSPs use the cyber threat information to better protect their customers, while OIs use the information to protect their internal networks. Once vetted, CSPs and OIs enter into a Memorandum of Agreement with the Department of Homeland Security to receive government furnished threat indicators. The indicators range in classification from Unclassified to Top Secret/SCI. The CSPs, such as AT&T, Century Link, Verizon, and Lockheed Martin, use the indicators to deliver Enhanced Cybersecurity Services to U.S.-based public and private entities through commercial relationships. The Enhanced Cybersecurity Services augment, not replace, existing cyber security capabilities operated by the entities.[30]

SHARING COORDINATION CHALLENGES

While obvious benefits exist in the sharing of cyber threat information, myriad coordination challenges must be considered. The first is the risk of disclosure of protective or detective capabilities and of sensitive information, such as personally identifiable information, intellectual property, trade secrets, or other proprietary information that can result in financial loss, legal action, or reputation damage. The second is the classification of information which might be difficult to actually use and expensive to request and maintain clearances for access. The third is trust in the use of the information, which can be time consuming to create and maintain. Next is the ability to consume the information through the infrastructure necessary to access external sources and to incorporate the information into the process for actual decisions. Fifth is the challenge of establishing interoperability for the secure, automated exchange of data among organizations, repositories, and tools. Ideally, the exchange would be through agreed upon formats and protocols. Finally, throughout the entire process of sharing information, is the challenge of preserving privacy of both individuals and organizations that may participate in sharing communities, but want their contributions to remain anonymous. Numerous technical initiatives and legal precedents are in the works or have been approved to remedy many of these coordination challenges.[31]

Sharing Legislation

After years of failed attempts to enact cybersecurity legislation, Congress passed the "Cybersecurity Act of 2015" on 18 December 2015 as part of an emergency budget omnibus bill. The Act is very similar to the "Cybersecurity Information Sharing Act (CISA)," which passed the Senate on 27 October 2015. President Obama signed the spending bill, enacting a $1.1 trillion budget and the Act with it. Title I of the Act, titled Cybersecurity Information Sharing, mandates the establishment of capabilities and procedures to facilitate and promote the timely sharing of cyber threat indicators, in addition to defensive measures between federal entities and non-federal entities. The procedures will require both entities, prior to sharing a cyber threat indicator, to remove personal information about a specific individual or information that identifies a specific individual not directly related to a cybersecurity threat. The Act provides an antitrust exemption, allowing two or more private entities to exchange or provide a cyber threat indicator or defensive measure relating to the prevention, investigation, or mitigation of a cybersecurity threat. It also provides protection from liability, such that "no cause of action shall lie or be maintained in any court against any private entity" for the monitoring of an information system and for the sharing or receipt of a cyber threat indicator or defensive measure.[32]

Passage of the Cybersecurity Act of 2015 required an intense sprint of negotiations. Privacy advocates say those late-night, closed-door negotiations removed hard-won protections. One major complaint is that cyber threat information will henceforth be shared directly with the National Security Agency. The original bill, CISA, was meant to allow companies to share information with other companies and the Department of Homeland Security, which would then filter it. Likewise, the purposes allowed under the negotiated bill for the government to disseminate data are criticized as being too broad. The allowed information is to be used to combat criminal activity, rather than being used for only cybersecurity.[33] Also, the final version of the enacted legislation calls on companies to remove information they "know" to be personal; earlier versions used the term they "reasonably believe."[34] Hill staffers acknowledged that the final bill wasn't the most pro-privacy version put forward, but it was the version that could pass Congress. To no surprise, a bipartisan group of privacy-minded and civil liberties-focused lawmakers sponsored a bill in January 2016 to repeal the Cybersecurity Act of 2015. Although the leader of the group, Representative Justin Amash (R-Michigan), called the beleaguered Act "the worst anti-privacy law since the USA Patriot Act,"[35] proponents argue that the enacted legislation was sorely needed to thwart the cyber attacks plaguing the public and private sectors.

Automated Mechanisms

Cyber threat intelligence should be shared in as close to real time as possible in order to block sequential attacks. Given this mandate, the Cybersecurity Act of 2015 imposed a 90-day deadline for the Secretary of Homeland Security, in coordination with the heads of appropriate Federal entities, to develop and implement a capability and process to commence real time, automated sharing of cyber threat indicators and defensive measures. The Department responded with deployment of their new Automated Indicator Sharing (AIS) system, which provides the capability for the timely exchange of relevant and actionable cyber threat indicators among federal departments and agencies and the private sector.[36] In this case, an indicator is defined as an observable, identified fact, plus a hypothesis about a threat. The goal of the AIS initiative is to enable the NCCIC to receive indicators from the private sector, remove unnecessary personally identifiable information, and disseminate the indicators. By design, the AIS initiative alleviates many challenges to sharing coordination. Specifically, it anonymizes the identity of the submitter, unless the submitter has consented to sharing its identity; minimizes the amount of data collected; retains information for a limited amount of time; and ensures that any collected information is used explicitly for authorized governmental purposes.[37]

Through the Automated Indicator Sharing effort, the DHS is building upon work already accomplished and adopted to the fullest extent possible, to include use of TAXII (Trusted Automated eXchange of Indicator Information) and STIX (Structured Threat Information eXchange) as core enabling technologies. TAXII is a means to send automated threat indicator messages, and STIX is a language to communicate those messages. TAXII defines a set of services and message exchanges that, when put in place, facilitates the sharing of actionable cyber threat information across organizational, product line, and service boundaries. TAXII is not itself an information sharing program and does not establish trust agreements, governance, or other non-technical facets of collaboration. Instead, TAXII helps organizations share selected information with the partners they choose. STIX is a collective effort to develop a standardized, structured language to characterize cyber threat information. The STIX framework aims to express the full range of potential cyber threat data elements. International in scope and free for public use, TAXII and STIX are community-driven technical specifications designed to permit automated information sharing for situational awareness, real-time network defense, and sophisticated threat analysis.[38]

IMPROVEMENTS LOOMING

The premise of sharing cyber threat intelligence is that attackers use the same tools and techniques on similar targets. In response, peer organizations can leverage observed and fused cyber threat information and indicators to identify and prevent subsequent attacks. Research by the Ponemon Institute indicates that 39 percent of attacks could be thwarted by threat intelligence sharing.[39] For example, the inclusion of external threat feeds into internal security platforms enhances behavioral (of system changes) and baseline (of abnormal events) anomaly detection methods.[40] However, the creation of an effective defense against advanced threats hinges not only on being able to detect intruders, but doing so in time to prevent damage to operations or assets. Therefore, the timely sharing of relevant and actionable cyber threat intelligence, in the context of cyber threat information and indicators, is imperative to reducing the impact of attacks. Organizations in the United States can turn to commercial sources or join sharing communities for various forms of cyber threat intelligence. The past three years have featured an explosion in new security firms offering cyber threat intelligence in the United States. Organizations have an array of commercial options when seeking to select an approach that combines quality and value.[41] They can also join a sector-based Information Sharing and Analysis Center or Organization, for which the latter structure is meant to extend information sharing across a region or in response to a specific, emerging threat.[42]

In the United States, the Secretary of Homeland Security has directed the accelerated deployment of technologies, guidance, and partnerships to enhance the Department's role in the cybersecurity of the government and the nation. Secretary Jeh Johnson recognized that "information sharing is fundamental to achieving our mission."[43] He expected that, in the near future, the Automated Indicator Sharing initiative would provide the capability to automate the distribution and receipt of cyber threat indicators. Improved Intelligence Community support to the resident

National Cybersecurity and Communications Integration Center will come from the fledgling Cyber Threat Intelligence Integration Center, enabling the ability to share more information with private sector partners. Still, challenges exist in sharing information between and among the private sector, particularly in privacy and trust. Although companies now have liability protection from new congressional legislation, their customers will not be notified that their data is being examined, and that data will be spread broadly across a thin patchwork of government IT systems,[44] vulnerable to intrusion, as seen in the breach of the Office of Personnel Management.[45] Yet, in regard to the ability to ‘‘share relevant information more quickly’’ and in a manner that ‘‘protects the privacy rights of all Americans,’’ President Obama’s cybersecurity coordinator, Michael Daniel, maintained: ‘‘These two things are not mutually exclusive—we can achieve both of those goals.’’[46] To hear an optimistic view on enacting the fundamental precept of cyber threat intelligence sharing is encouraging.

REFERENCES

[1] Dell SecureWorks, ‘‘Underground Hacker Markets,’’ White Paper, December 2014, pp. 1–14.

[2] CrowdStrike, ‘‘2015 Global Threat Report,’’ February 2016, pp. 12–13.

[3] Kaspersky Lab, ‘‘Cyber Attacks Mean Bill Bills for Business,’’ Worldwide Survey of 5,500 Companies, 2015, p. 1.

[4] Threat Connect, ‘‘Threat Intelligence Platforms,’’ White Paper, 2015, pp. 1–11.

[5] Verizon, ‘‘2015 Data Breach Investigations Report,’’ June 2015, p. 11.

[6] Solutionary, ‘‘2015 NTT Group Global Threat Intelligence Report,’’ 2015, pp. 49–50.

[7] Solutionary, ‘‘Threat Intelligence Defined,’’ White Paper, 2015, pp. 6–13.

[8] National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing (Draft),* Special Publication 800–150 (Draft), (Washington, DC: U.S. Department of Commerce, October 2014), pp. 11–13.

[9] Crowdstrike, ‘‘Indicators of Attack versus Indicators of Compromise,’’ White Paper, 2015, pp. 1–10.

[10] SANS, Dave Shackleford, ‘‘Who’s Using Cyberthreat Intelligence and How?,’’ A SANS Survey, February 2015, pp. 1–14.

[11] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800–61, Revision 2 (Washington, DC: U.S. Department of Commerce), August 2012, pp. 27–28.

[12] VirusTotal, ‘‘Putting the Spotlight on Firmware Malware,’’ at www.virustotal.com, 27 January 2016.

[13] Palo Alto Networks, ‘‘3 Ways to Counter Multi-Vector Attacks,’’ posted by Karin Shopen, at www.researchcenter.paloaltonetworks.com, 8 February 2016.

[14] Bob Gourley, *The Cyber Threat* (Create Space Independent Publishing Platform, 23 September 2014), Appendix 2, pp. 81–84.

[15] McAfee, "McAfee Global Threat Intelligence: Turn It On," White Paper, 2010, pp. 1–23.

[16] FireEye, "FireEye Threat Intelligence: Get the Intelligence and Context You Need to Help Identify, Block and Respond to Advanced Attacks," Data Sheet, 2015, pp. 1–4.

[17] LookingGlass, "Virus Tracker: Global Threat Network Feed Source," Product Listing, www.lgscout.com/products/virus-tracker/, March 21, 2016.

[18] Executive Office of the President, *Presidential Policy Directive on Critical Infrastructure Protection*, PPD-63 (Washington, DC: The White House, 12 February 2013).

[19] National Council of ISACs, "Information Sharing and Analysis Centers (ISACs) and their Role in Critical Infrastructure Protection," January 2016, p. 2.

[20] National Council of ISACs, "Join Your Sector's Information Sharing and Analysis Center," January 2016, p. 2.

[21] The White House, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," Stanford University, 13 February 2015.

[22] Executive Office of the President, *Executive Order—Promoting Private Sector Cybersecurity Information Sharing* (Washington, DC: The White House, 13 February 2015).

[23] Scott Algeier, Remarks at the ISAC/ISAO Summit, 4 March 2015.

[24] United States Computer Emergency Readiness Team, "National Cybersecurity and Communications Integration Center," Official Website of the Department of Homeland Security, accessed on 23 February 2016.

[25] DHS Press Office, "Statement by Deputy Secretary Alejandro Mayorkas on the Cyber Threat Intelligence Integration Center," Official Website of the Department of Homeland Security, 7 January 2016.

[26] The White House, "Cyber Threat Intelligence Integration Center," Fact Sheet, 25 February 2015.

[27] Mark Pomerleau, "New Cyber Center to Focus on Collecting Data, Analyzing Threats," *Defense Systems*, March/April 2015, p. 26.

[28] Ashley Carman, "White House Criticizes Bill Clarifying Cyber Threat Intelligence Integration Center Missions," *SC Magazine*, 22 June 2015.

[29] Department of Homeland Security, "Critical Infrastructure Key Resources (CIKR) Cyber Information Sharing and Collaboration Program," Fact Sheet, 3 February 2016, pp. 1–2.

[30] Department of Homeland Security, "Enhanced Cybersecurity Services," Fact Sheet, 3 February 2016, pp. 1–2.

[31] National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing* (*Draft*), pp. 8–9.

[32] U.S. Congress, "Consolidated Appropriations Act, 2016," Division N-Cybersecurity Act of 2015, 15 December 2015, pp. 1728–1770.

[33] Michael Heller, "CISA Added to Budget Omnibus, with Privacy Protection Stripped," *Tech Target*, 18 December 2015.

[34] Tal Kopan, "Obama to Sign Cybersecurity Bill as Privacy Advocates Fume," *CNN Politics*, 18 December 2015.

[35] Cory Bennett, "Amash Bill would Repeal New Cybersecurity Law," *The Hill*, 14 January 2016.

[36] Bradley Barth, "DHS launches two-way threat sharing system for public-private collaboration," *SC Magazine*, March 18, 2016.

[37] United States Computer Emergency Readiness Team, "Automated Indicator Sharing (AIS)," Official Website of the Department of Homeland Security, accessed 23 February 2016.

[38] United States Computer Emergency Readiness Team, "Information Sharing Specifications for Cybersecurity," Official Website of the Department of Homeland Security, accessed on 23 February 2016.

[39] Ponemon Institute, "Flipping the Economics of Attacks," 26 January 2016.

[40] Ramses Gallego, "Security Think Tank: Security Intelligence is Useful only if Isolated from the Noise," *Computer Weekly*, 25 February 2016.

[41] Digital Shadows, "Cyber Threat Intelligence: A Buyer's Guide," White Paper, 2016, pp. 1–22.

[42] Vincent Voci, "Five Takeaways From the ISAO Conference," U.S. Chamber of Commerce, 18 February 2016.

[43] Jeh Charles Johnson, "Worldwide Threats and Homeland Security Challenges," prepared testimony before the House Committee on Homeland Security, 21 October 2015.

[44] Sam Thielman, "Senate Passes Controversial Cybersecurity Bill CISA 74–21," *The Guardian*, 27 October 2015.

[45] Kirstin Finklea, "Cyber Intrusion into U.S. Office of Personnel Management: In Brief," Congressional Research Service, CRS Report R44111, 17 July 2015.

[46] Billy Mitchell, "White House Renews Push to Pass CISA," *Fedscoop*, 6 October 2015.