FIU Law Review

Volume 10 | Number 2 Article 16

Spring 2015

Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector

Scott J. Shackelford
Indiana University

Scott Russell J.D.
Center for Applied Cybersecurity Research

Online ISSN: 2643-7759

Recommended Citation
Scott J. Shackelford & Scott Russell J.D., *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FIU L. Rev. 635 (2015).
DOI: https://dx.doi.org/10.25148/lawrev.10.2.16

Above the Cloud:
Enhancing Cybersecurity in the Aerospace Sector

Scott J. Shackelford, J.D., Ph.D.[*] *& Scott Russell, J.D.*[**]

ABSTRACT

Congressional testimony shows that NASA's Jet Propulsion Lab was under sustained cyber attacks for years. Yet this episode was only part of a string of some thirteen successful breaches in 2011 alone, prompting an investigation by the NASA Office of Inspector General, which stated: "We found that computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet." The report goes on to note, "[t]hese deficiencies occurred because NASA had not fully assessed and mitigated risks to its Agency-wide mission network and was slow to assign responsibility for IT security oversight to ensure the network was adequately protected." Yet NASA is far from the only victim in the air and space sector of cyber attacks. Organizations ranging from defense contractors like Lockheed Martin to SpaceX have been targeted, and sometimes penetrated, resulting in the loss of invaluable trade secrets that impact economic competitiveness and national security alike. This Article argues that a polycentric response is needed to manage the cyber threat to the aerospace sector. As part of this approach, aerospace organizations should utilize the recently released National Institute for Standards and Technology Cybersecurity Framework to better protect their assets by instilling cybersecurity best practices from the bottom up, and should engage in more robust information sharing, similar to recent efforts in the critical infrastructure and retail sectors.

---

* Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution.

** Post-Graduate Fellow, Center for Applied Cybersecurity Research.

INTRODUCTION

NASA's Jet Propulsion Laboratory was under sustained cyber attacks for years, according to Congressional testimony.[1] Yet this incident was only part of a string of some thirteen successful NASA breaches in 2011 alone,[2] prompting an investigation by the NASA Office of Inspector General. Following an investigation by the NASA Office of the Inspector General, the Officer released a report that stated: "We found that computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet."[3] The report further notes, "[t]hese deficiencies occurred because NASA had not fully assessed and mitigated risks to its Agency-wide mission network and was slow to assign responsibility for IT security oversight to ensure the network was adequately protected."[4] Yet NASA is far from the only cyber attack victim in the aerospace sector. Organizations ranging from defense contractors like

---

[1] Marc Boucher, *NASA Has Been under Heavy Cyber Attack*, NASA WATCH (Mar. 5, 2013, 7:36 AM), http://nasawatch.com/archives/2013/03/nasa-has-been-u.html.

[2] *See* Emil Protalinski, *NASA: Hackers Had 'Full Functional Control',* ZDNET (Mar. 2, 2012), http://www.zdnet.com/blog/security/nasa-hackers-had-full-functional-control/10443.

[3] NASA OFF. INSPECTOR GEN., INADEQUATE SECURITY PRACTICES EXPOSE KEY NASA NETWORK TO CYBER ATTACK (2011), http://oig.nasa.gov/audits/reports/FY11/IG-11-017.pdf.

[4] *Id.*

Lockheed Martin to product manufacturers like Space Exploration Technologies Corporation (SpaceX) have been targeted, and sometimes penetrated, resulting in the loss of valuable trade secrets that impact economic competitiveness and national security alike.[5] This Article argues that a "polycentric" response is needed to manage the cyber threat to the aerospace sector.[6] As part of this approach, aerospace organizations should utilize the recently released National Institute for Standards and Technology (NIST) Cybersecurity Framework to better protect their assets by instilling cybersecurity best practices from the bottom up,[7] as well as engaging in more robust information sharing similar to recent efforts in the critical infrastructure and retail sectors.[8]

This Article is structured as follows. Part I begins the analysis by breaking down the multifaceted cyber threat to critical infrastructure generally before focusing on the issue of protecting trade secrets in the aerospace sector. Case studies on effective and ineffective cybersecurity management are offered that include surveying the likes of Boeing and NASA.[9] Part II then pivots to the regulatory landscape discussing applicable U.S., European Union, and international laws for securing trade secrets, with special emphasis on the NIST Cybersecurity Framework, which is comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[10] Finally, Part III makes the case for a proactive approach to identifying and instilling the best

---

5 *See*, *e.g.*, Siobhan Gorman, August Cole & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009, 12:01 AM), http://online.wsj.com/article/SB124027491029837401.html; Andrea Tse, *See What Elon Musk's Right Hand Man Has to Say About Cyber Hackers*, THE ST. (Feb. 25, 2014, 2:57 PM), *available at* http://www.thestreet.com/story/12441320/1/see-what-elon-musks-right-hand-man-has-to-say-about-cyber-hackers.html.

6 *See* Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* (2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

7 NAT'L INST. STAN. & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VER. 1.0, at 1 (2014) [hereinafter NIST CYBERSECURITY FRAMEWORK].

8 The aviation sector planned such an information-sharing organization to launch in September 2014, which, we argue, should expand to the aerospace sector writ large. *See Aviation Info-Sharing Body Refining Structure Before September Launch*, INSIDE CYBERSECURITY (July 16, 2014), http://alturl.com/9roi9.

9 These two case studies were chosen given that they represent leading public- and private-sector entities in the aerospace sector. Other organizations such as SpaceX would be invaluable to focus on as well, but unfortunately not enough public information exists that we could locate to warrant in-depth analysis.

10 *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), *available at* http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

cybersecurity practices throughout the aerospace sector as part of a "polycentric" approach to fostering cyber peace.

I. THE CYBER THREAT TO THE AEROSPACE SECTOR

To put it plainly, space, particularly commercial space, is a big deal. Commercial spending in space surpassed $250 billion in 2008.[11] NASA officials endorse this private sector interest, with former NASA Administrator Michael Griffin stating, "[s]ooner rather than later, government space activity must become a lesser rather than a greater part of what it is that humans do in space."[12] Yet, even as the private sector emerges as a key player in space, other stakeholders including nations are reassessing, and in some cases reasserting space policies.[13] The final frontier is getting more crowded thanks to increased national attention on space exploration, heightened private-sector interest, and the intensified use of cyberspace to provide new opportunities for space commerce.[14] The intersection of these forces has provided fertile ground for a multitude of public-and private-sector actors to leverage the new tools of cyberspace, including cyber attacks, to gain commercial and national security advantages.[15] This Part explores the evolution of the cyber threat to the aerospace sector focusing on trade secret theft and introduces the implications of the aerospace sector being designated as one component of U.S. critical national infrastructure.

A. Breaking Down the Cyber Threat to Critical Infrastructure

According to a 2009 McAfee/CSIS report, "[c]ritical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often by high-level adversaries [such as foreign governments]."[16] Indeed, some utilities have reported being probed

---

11 *See* SPACE FOUNDATION, THE SPACE REPORT 2008: THE AUTHORITATIVE GUIDE TO GLOBAL SPACE ACTIVITY 1-2 (2008) [hereinafter THE SPACE REPORT]. Recent developments such as U.S.-based SpaceX successful resupply mission to the ISS underscore this trend. *See, e.g.*, Frank Morring, Jr., *SpaceX Success Gives Commercial Spaceflight a Boost*, AVIATION WK. (June 18, 2012), http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_06_18_2012_p26-466690.xml.

12 MICHAEL GRIFFIN, REMARKS AT CTR. FOR STRATEGIC & INT'L STUD., WORKSHOP ON SPACE EXPLORATION AND INTERNATIONAL COOPERATION 1 (Nov. 1, 2005), *available at* www.nasa.gov/pdf/137173main_mg_csis.pdf.

13 *See* Scott J. Shackelford, *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 AM. BUS. L.J. 429, 430–35 (2014) (exploring the evolution of space commerce along with the use of polycentric governance to mitigate threats to its development, including orbital debris).

14 *See id.*

15 *See infra* notes 1–5.

16 IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR, MCAFEE/CSIS 1 (2009), http://iom.invensys.com/EN/pdfLibrary/McAfee/WP_McAfee_In_The_Crossfire_03-10.pdf

thousands of times per month.[17] These figures point to the various dimensions of the cyber threat facing the private-sector, which are often broken down into cyber war, crime, espionage, and terrorism. However, given the overlap in these categories and our focus on critical infrastructure, of particular relevance is the management of cyber attacks below the armed attack threshold – namely, cybercrime and espionage.[18]

Defending critical infrastructure (CI) against the threat posed by cyber attacks has been of increasing interest to governments the world over, but vexing given the need for active private-sector involvement in an arena where the vast majority of CI is privately operated.[19] In 2009, soon after taking office, President Obama ordered a systemic review of U.S. cybersecurity in critical infrastructure,[20] which concluded that cybersecurity was a "strategic national asset" leading to the creation of the U.S. Cyber Command (CYBERCOM): the military command tasked with oversight of U.S. cybersecurity for the dot-mil domain.[21] Yet this development is notable as much for what it leaves out as for what it protects. Maintaining adequate cybersecurity across the spectrum of U.S. critical infrastructure has proven to be a herculean task that, to this day, has not been adequately addressed, though the NIST Cybersecurity Framework referenced above and discussed further below does show some promise.[22]

Despite wide consensus that the protection of CI generally should be a priority, there is less clarity as to the scope of what exactly constitutes CI. At a high level of abstraction, CI may be considered all "systems and assets, whether physical or virtual, so vital . . . that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[23] Such was the definition of CI in the

---

[hereinafter IN THE CROSSFIRE].

17 MCAFEE & CSIS, IN THE DARK: CRITICAL INDUSTRIES CONFRONTING CYBERATTACKS 5 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

18 For more on this distinction, see Chapter 1 of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

19 *See, e.g.*, Bruce McConnell, *Working Together to Strengthen the Nation's Critical Infrastructure*, DHS (May 2, 2013), http://www.dhs.gov/blog/2013/05/02/working-together-strengthen-nation%E2%80%99s-critical-infrastructure.

20 *See* Roy Mark, *Obama Orders 60-Day Cyber-Security Review*, EWEEK (Feb. 2, 2010), http://www.eweek.com/c/a/Security/Obama-Orders-60Day-Cyber-Security-Review/.

21 *See* Press Release, U.S. DEP'T OF DEFENSE, DOD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander (May 21, 2010), http://www.defense.gov/releases/release.aspx?releaseid=13551.

22 *See, e.g.*, Jeremy Broggi, *Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes,* 37 HARV. J.L. & PUB. POL'Y 653 (2014).

23 Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195(e) (2012).

Critical Infrastructure Protection Act of 2001.[24] Yet this definition provides little practical clarity to the issue and is articulated so broadly that nearly every industry could be considered "critical." To help address this situation, Presidential Policy Directive 21 identifies sixteen sectors, ranging from energy to manufacturing to financial services, that are deemed "critical infrastructure."[25] Although aerospace is not mentioned *per se* in this list, the fact that both the "defense industrial base" and "transportation systems" are mentioned makes it likely that aerospace would in fact be included in this CI regulation.[26]

Notwithstanding the Critical Infrastructure Protection Act of 2001, in practice CI oversight is distributed between various agencies based on the specific sector in play, e.g., the Environmental Protection Agency covers the water supply, while the Department of the Treasury handles finance.[27] As such, CI protection in the United States is a piecemeal collection of myriad regulations with numerous overlapping regulatory bodies, each with distinct systems, methods, priorities, and goals.[28] This sector-specific approach (unlike the situation in Europe, as is discussed in Part II), though, misses the fact that by its nature CI is interconnected. A failure in the electrical grid would impact public health, communications, and defense, to name only a few sectors. This inherent interconnectivity makes CI uniquely vulnerable to cyber attacks.[29] Since most every CI sector relies on the Internet or computer networks, each is a potential target for cyber attacks.[30] Therefore, robust cybersecurity in one sector could still be undermined by

---

24 *Id.*

25 OFFICE OF THE PRESS SEC'Y, PRESIDENTIAL POLICY DIRECTIVE 21: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; *see also What Is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure (last visited Jan. 16, 2014); *What Is the ICS-CERT Mission?*, http://ics-cert.us-cert.gov/Frequently-Asked-Questions (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems.).

26 *See What Is Critical Infrastructure*, *supra* note 25.

27 *Id.*

28 *See, e.g.*, William Jackson, *Industry Needs Government Help to Protect Infrastructure, GAO Study Says*, GCN (Jan. 10, 2012), http://gcn.com/articles/2012/01/10/critical-infrastructure-protection-gao.aspx ("U.S. critical infrastructure protection is a patchwork process depending primarily on voluntary public- and private-sector cooperation that could leave large portions inadequately protected, according to a recent study by the Government Accountability Office.").

29 *See U.S. Intelligence Cmty. Worldwide Threat Assessment: Statement for the Rec. Before S. Select Comm. on Intelligence*, 113th Cong. 1-2 (2013) (statement of James R. Clapper, Director of National Intelligence).

30 *Id.*

another sector's vulnerability.[31] The proverbial "weak link" in the chain of CI could result in catastrophic economic damage, which is compounded by the sheer number of access points that cyber attackers may exploit. Government contractors, private-sector actors, public-sector organizations, utilities companies, and so on, all have separate regulators, differing cybersecurity standards, and long supply chains.[32] Taking the latter point, the underlying networks are composed of countless hardware components produced all over the globe, each creating potential security problems that must be assessed and, if necessary, rectified.[33] For instance, the Boeing 777 airplane consists of over three million parts produced by 500 suppliers from all over the globe.[34] Yet from a security standpoint, Boeing must verify each of these prior to incorporating them into the final product, as vulnerabilities in key components can sabotage the entire enterprise. That is far easier said than done, as may be seen by reports that the satellite communications systems that passenger jets rely on are vulnerable to cyber attacks "through their WiFi and inflight entertainment systems."[35]

The problem of securing vulnerable supply chains is so pervasive that regulators from around the world have tried various schemes to improve the unacceptable status quo. The Chinese government, for example, implemented a "multi-level protection scheme," with industries classified above a three (on a scale of one to five) required to source components from Chinese state-affiliated companies and more broadly utilize Chinese IP.[36] While such a command-and-control type regulation is unlikely to emerge in the United States in the foreseeable future, the U.S. government has restricted the utilization of component parts made by the two largest Chinese telecommunications providers, Huawei and ZTE.[37] Furthermore, the NIST Cybersecurity Framework emphasizes "Asset Management," or that the "data, personal devices, systems, and facilities . . . are managed consistent with their relative importance . . . and the organization's risk

---

31 *Id.*

32 *See* GCN, *supra* note 28; John Villasenor, *Ensuring Hardware Cybersecurity*, BROOKINGS INST. (May 2011), http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity.

33 *See id.*; Bryan Krekel et al., *Chinese Capabilities for Computer Network Operations and Cyber Espionage*, WASH. POST (Mar. 7, 2012), http://tinyurl.com/7wsyte3.

34 *Boeing 777 Facts*, BOEING, http://www.boeing.com/boeing/commercial/777family/pf/pf_facts.page (last visited Oct. 7, 2014).

35 Jim Finkle, *Hacker Says to Show Passenger Jets at Risk of Cyber Attacks*, REUTERS (Aug. 4, 2014), http://www.reuters.com/article/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804.

36 *See* Nathaniel Ahrens, *Of Shoes, Buttons, and Routers*, CSIS (Nov. 8, 2012), http://csis.org/publication/national-security-and-chinas-information-security-standards.

37 STAFF OF PERMANENT SELECT COMM. ON INTELLIGENCE, 112th CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE, at vi (Oct. 8, 2012), http://tinyurl.com/pmuf5he.

strategy."[38] This highlights the fact that the U.S. government is working to develop a standard among private sector actors that emphasizes the need to identify the cyber risk presented by the scope and breadth of their business operations, along with the need to take appropriate actions to mitigate that risk.[39] For example, in the aerospace context although planes may be the targets of cyber attacks,[40] so too might the systems on which the planes rely. A 2010 governmental review found cyber attack vulnerabilities in the Federal Aviation Administration (FAA) were due in part to outdated equipment usage by the air traffic control facilities.[41] In this highly networked and visible arena, the threat of cyberterrorism to aviation in particular is heightened.[42]

Although discussions of CI security often involve speculation about debilitating cyber attacks that could cripple U.S. CI, in many ways the more pervasive and pressing concern, particularly to the aerospace sector, comes from the theft of trade secrets.[43] Intelligence operations aside, cyber criminals are unlikely to perpetrate a doomsday attack on CI since it is much more profitable to slowly leach intellectual property from firms without risking a dramatic change in the regulatory or prosecutorial landscape. It is to that topic that we turn to next.

B. Trade Secrets Theft

A trade secret may be defined in the U.S. context as "any confidential business information which provides an enterprise a competitive edge" and is not publicly known.[44] Examples include formulas, sales methods, and

---

38 NIST CYBERSECURITY FRAMEWORK, *supra* note 7, at 1.

39 *See id.*

40 Kim Zetter, *FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack*, WIRED (Jan. 4, 2008), http:// www.wired.com/politics/security/news/2008/01/dreamliner_security.

41 Lolita C. Baldor, *Cyber Security Still Issue for FAA*, BOSTON GLOBE (Aug. 13, 2010), http:// www.boston.com/news/nation/washington/articles/2010/08/13/cyber_security_still_ issue_for_faa.

42 Ruwantissa Abeyratne, *Cyberterrorism: The Next Great Threat to Aviation*, 24 AIR & SPACE L. 4, 4–6 (2011).

43 *See* Ellen Nakashima, *White House Launches Effort to Deter Theft of Trade Secrets*, WASH. POST, Feb. 21, 2013, at A11.

44 *What is a Trade Secret?*, WIPO, http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_ secrets.htm (last visited May 6, 2014); *see also* 18 U.S.C. § 1839(3) (2012) ("[T]the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.").

industrial processes.[45] Trade secret theft is becoming increasingly common and extremely costly. Estimated losses caused by alleged Chinese trade secrets misappropriation alone were approximately $1.1 billion in 2011.[46] Trade secrets are appealing to businesses for many reasons, including the relatively low cost to obtain protection,[47] the potentially broad subject matter that may be protected, and the theoretically unlimited protection period (unlike, for example, the limited protection period offered by patents).[48] Yet this low barrier-to-entry comes with greater fragility; disclosing secret information destroys the existence of a remedy, making trade secrets independently discoverable by third parties (and potentially patented), and seeking redress from the theft of trade secrets is often difficult and may result in inadequate compensation for the victim even if proven.[49]

It is easy to see why cyber criminals are so attracted to trade secrets; while credit card numbers may fetch pennies on the black market, valuable trade secrets still command a premium.[50] Moreover, given the increasing prevalence of cloud computing, mobile devices, distributed networks, telecommuting, and the "Internet of things," the number of breach points has escalated exponentially.[51] And since a significant percentage of trade secret theft is allegedly perpetrated internationally, there are the added protections of ambiguous national and international laws relating to

---

45 The Uniform Trade Secrets Act, which generally is followed by local authorities within the United States, defines a trade secret as information that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other person who can obtain economic value from its disclosure or use, and; (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. § 1(4)(i)–(ii) (codified as amended at 14 U.L.A. 438 (1985), *available at* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. This definition is reinforced by the Restatement (Third) of Unfair Competition, which defines a trade secret as "any information that can be used in the operation of a business or other enterprise that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

46 *See* U.S. INT'L TRADE COMM'N, PUB. NO. 4226, CHINA: EFFECTS OF INTELLECTUAL PROPERTY INFRINGEMENT AND INDIGENOUS INNOVATION POLICIES ON THE U.S. ECONOMY 3-42 (2011), *available at* http://www.usitc.gov/publications/332/pub4226.pdf (reporting 2009 estimates).

47 *See* Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secrets Rights in Response to Cyber-Misappropriation*, 16 YALE J. L. & TECH. 172, 175 (2014).

48 *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 494 (1974) (Marshall, J., concurring) (noting that trade secret law offers protection of unlimited duration).

49 *See* Argento, *supra* note 47, at 186.

50 *See* David S. Almeling, *Seven Reasons Why Trade Secrets are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104–06 (2012).

51 OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2009–2011 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_ 2011.pdf.

enforcement and extradition.[52] Indeed, the relative ease and safety of trade secret theft is such that certain governments are believed to use this practice as an integral part of their domestic economic policies.[53]

U.S. trade secret law is something of a hodgepodge of federal criminal laws, state criminal laws, and state civil actions.[54] The majority of litigation around U.S. trade secrets arises in the context of state civil litigation.[55] Among the states, all but three have adopted some form of the Uniform Trade Secrets Act (UTSA), and despite some discussion on the issue, it is widely acknowledged that the UTSA encompasses both the theft of trade secrets by hacking and the misappropriation of trade secrets by company insiders via computers.[56]

International trade secret protection is even more varied. Despite relatively widespread acceptance of what constitutes a trade secret, the scope of protection varies by nation.[57] Although trade secrets are included in the TRIPS agreement under Article 39, for example, the specific guidelines for how countries should implement trade secret protection is left to the individual countries' determinations.[58] Therefore, trade secret protection may be left to other mechanisms to satisfy enforcement internationally, such as bilateral investment treaties.[59] Regardless, given difficulties surrounding the definition, protection, and prosecution of trade secret claims, firms would be well-advised to enact proactive cybersecurity stances as is discussed in Part III. But the extent to which aerospace organizations in particular are taking this advice varies by organization, as is discussed in the next section.

---

52 *See* Aaron J. Burstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933, 944–46 (2009).

53 MANDIANT, APT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 21 (Jan. 2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_ Report.pdf.

54 *See* MELVIN F. JAGER, TRADE SECRETS LAW § 2.3 (2013).

55 David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 45 GONZ. L. REV. 291, 306 (2010-2011).

56 *See, e.g.*, Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions,* U. ILL. J.L. TECH. & POL'Y 429, 442-45 (2009) (discussing disunity between trade secret misappropriation under the UTSA and unauthorized access of a protected computer under the CFAA).

57 *See* Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1 (2014).

58 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, *available at* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm.

59 *See* Shackelford et al., *supra* note 57.

C. Case Studies in Aerospace Cybersecurity

This section uses examples from the aerospace giants Boeing and NASA to highlight cybersecurity practices before moving on to discuss the applicable regulatory environment in greater detail in Part II. We pay particular attention to security lapses by these sophisticated actors since it demonstrates the difficulty of effectively managing cyber risk.

1. Boeing's Breach

As an example of a recent aerospace security breach and its aftermath, consider the recently revealed cyber attack on Boeing. The company was subjected to a prolonged and sophisticated cyber attack beginning in 2009, resulting in the loss of potentially millions of dollars in trade secrets relating to the C17 Military transport.[60] Three Chinese nationals perpetrated the attack, with at least one operating out of Canada.[61] Over the course of some four years, they obtained more than sixty-five gigabytes of data, and were only discovered through FBI investigation.[62] Perhaps more striking than the quantity of data lost was the hackers' discussion of the complexity and sophistication of Boeing's cybersecurity defenses. In an internal email, the hackers debate Boeing's various firewalls, intruder prevention and detection systems, and file transfer defenses.[63] They showed a substantial familiarity with the architecture of Boeing's networks and acted both slowly and with "meticulous planning and vigorous technical support."[64] In short, despite Boeing's efforts, a team of three savvy criminals was able to penetrate one of the most sophisticated aerospace firms in the world. And, it did not take a rare zero-day exploit flaw or advanced persistent threat; just an email.[65]

Despite the aforementioned "vigorous technical support" and funding, Boeing, like Lockheed Martin and other aerospace firms, ultimately fell prey to a phishing email.[66] Phishing emails are targeted attacks wherein the target is induced to open an attachment or click on a link, which would then grant the assailant control over the computer.[67] Although these exploits have been used for some time, they are becoming more sophisticated and

---

60 Criminal Complaint, *United States v. Su Bin*, NO. 14-1318M, (CDCA, June 27, 2014), *available at* https://www.documentcloud.org/documents/1216505-su-bin-u-s-district-court-complaint-june-27-2014.html.

61 *Id.*

62 *Id.*

63 *Id.*

64 *Id.* at 23.

65 *Id.*

66 *Id.* at 11.

67 Tom N. Jagatic et al., *Social Phishing*, 50 COMM. ACM 94, 94–95 (2007).

successful, even fooling the likes of Google employees in 2009.[68] According to *The Economist*, "The amount of information now available online about individuals makes it ever easier to attack a computer by crafting a personalized email that is more likely to be trusted and opened."[69] From the email correspondence used to indict Su Bin, (one of the three hackers), it appears that he initially obtained a document containing the contact information of a large number of contractors and military personnel, and from there he was able to select the vectors for his targeted attacks.[70] This suggests that it is still the human element of system security that is the weakest link in an insecure chain.

The hackers' techniques in the Boeing breach highlight the sophistication that can be employed in targeted cyber attacks on aerospace firms. They utilized jump servers, also called "hop points," to route their attacks through at least three other countries and ensured that at least one of the countries "did not have friendly relations with the U.S."[71] In so doing, the hackers took advantage of technical, legal, and geopolitical hurdles that companies must manage when protecting against cyber threats. The hackers were highly familiar with the traditional cybersecurity defenses utilized by Boeing and organized their attack such that they avoided honeypots, transfer restrictions, and traditional time-based access restrictions.[72]

This Boeing assault identifies numerous challenges faced by large aerospace firms. It illustrates that firms must be aware of their place within the cyber threat matrix and that for multinationals, this includes protecting themselves from the most sophisticated actors, namely nation states. This necessitates staying on the cutting edge of cybersecurity best practices discussed in Part III, which the NIST Cybersecurity Framework combined with robust private-private, public-private, and private-public information sharing may help facilitate.

2. Network Defense at NASA

Like Boeing, and as was discussed in the Introduction, NASA has had its fair share of cybersecurity lapses. In 2010 and 2011 alone, NASA self-reported more than 5,000 *successful* cyber attacks.[73] In fact, the problem grew to such an extent that NASA's Inspector General had to get involved, issuing a report to Congress in 2011 that, among other things, cited the

---

68 *Spear Phishers: Angling to Steal Your Financial Info*, FBI (Apr. 1, 2009), http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

69 *See*, *e.g.*, *Cyberwar: War in the Fifth Domain*, 25 ECONOMIST (July 3, 2010).

70 *United States v. Su Bin*, *supra* note 60, at 20.

71 *Id.* at 24.

72 *Id.* at 22–23.

73 NASA OFF. INSPECTOR GEN., *supra* note 3, at 1.

agency for the: "Lack of full awareness of [the] Agency-wide IT security posture . . . [the] [s]low pace of encryption for NASA laptop computers and other mobile devices . . . [and the lack of] [a]bility to combat sophisticated cyber attacks . . . ."[74] Yet also like Boeing, NASA faces a difficult problem in getting its cyber house in order. The Agency is responsible for some "550 information systems that control spacecraft, collect and process scientific data, and enable NASA personnel to collaborate with colleagues around the world."[75] Moreover, these systems are not closed proprietary networks, but instead are open to contractors and even the general public.[76]

The total cost of NASA's breaches is unknown, but given its status as a "target rich" environment rife with valuable trade secrets of which foreign governments and aerospace firms would be interested, the necessity of proactively defending NASA's networks is manifest.[77] Although there is a range of potential topics to discuss in this realm, we focus on just two, budgeting and organization, as a springboard for our discussion of cybersecurity best practices in Part III. First, out of NASA's more than $18 billion budget for FY 2011, it spent more than $1.5 billion (or 8.3 percent) of its budget on "IT-related activities."[78] Yet just $58 million of that amount went to cybersecurity, which works out to 4 percent of NASA's IT budget.[79] The U.S. government, for comparison's sake, spends roughly 11 percent of its public IT budget on cybersecurity, according to Booz Allen.[80] Although it is not as simple as spending one's way to cybersecurity, since infinite investment does not breed infinite security, such a rebalancing could help as NASA seeks to re-launch its cybersecurity efforts.

Second, a key finding of the 2011 NASA IG report is that NASA needs a Chief Information Officer who enjoys both visibility and oversight authority over all the agency's cybersecurity efforts.[81] This finding is consistent with the literature and should be of interest to aerospace firms generally. Indeed, it is vital to create a "centralized management of IT security solutions" such that there is an automatic mechanism for measuring

---

74 *Id.*

75 *Id.*

76 *Id.*

77 *See, e.g.*, Nicole Perlroth, *2nd China Army Unit Implicated in Online Spying*, N.Y. TIMES (June 9, 2014), http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0.

78 NASA OFF. INSPECTOR GEN., *supra* note 3, at 1.

79 *Id.*

80 *See Cyber Management*, BOOZ ALLEN HAMILTON at 1, www.boozallen.com/media/file/cyber-management.pdf (last visited Jan. 9, 2013) (reporting that "[t]he U.S. spends $80 billion per year on information and communications technology—$9 billion of which goes into information technology (IT) security").

81 NASA OFF. INSPECTOR GEN., *supra* note 3, at 2.

and enforcing IT security best practices throughout an organization.[82] Chief Information Security Officers (CISOs) are one way to achieve such coordination as they enable "enterprises to align information protection with corporate security policies and regulatory or business-partner mandates."[83] Companies with CISOs have saved more than twenty percent on the cost of data breaches over those that do not have those management figures in place, according to one Symantec survey.[84] Firms are increasingly recognizing this need. In 2006, only forty-three percent of respondents to a PwC survey said that they had a CISO or other similar security executive, but by 2009, that rate had increased to 85 percent.[85] NASA now has a CIO for IT Security,[86] which should help enhance the agency's cybersecurity efforts.

D. Summary

This Part has introduced the multifaceted cyber threat facing aerospace organizations, discussed some of the applicable regulatory regimes surrounding CI and trade secrets and ran through two case studies in aerospace cybersecurity defense. The next Part digs deeper into the applicable regulatory landscape not just in the United States, but globally including the European Union, paying particular attention to CI regulations shaping the legal environment for aerospace firms.

II. THE REGULATORY LANDSCAPE

Sometimes the biggest breaches begin with the smallest of actions. Consider the sequence of events that were initiated when a man opened an email entitled "2011 Recruitment Plan" in late 2011.[87] He unintentionally allowed "hackers to raid the computer networks of his employer, RSA[,]" whose cybersecurity products help protect the networks of the U.S. government and many Fortune 500 companies.[88] According to U.S. General Keith Alexander, former National Security Agency director and commander of CYBERCOM, blame for the breach lay with an organized campaign

---

82 ANNUAL STUDY: U.S. COST OF A DATA BREACH, PONEMON INST. 8 (2010), http://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf.

83 *Id.*

84 *Id.* at 32.

85 Ralph DeFragesco, *Chief Information Security Officer: A New Spin on an Old Job*, IT BUS. EDGE (Nov. 2, 2009), http://www.itbusinessedge.com/cm/blogs/defrangesco/chief-information-security-officer-a-new-spin-on-an-old-job/?cs=37172.

86 *See IT Sec. Div.*, NASA, http://www.nasa.gov/offices/ocio/itsecurity/#.VDLFf-d9nS0 (last visited Oct. 7, 2014).

87 Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR (Sept. 2011), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109/.

88 GRIFFIN, *supra* note 12.

orchestrated by elements within China.[89] Among the companies targeted in the aftermath of the breach was Lockheed Martin, which reportedly lost "data on the F-35 Lightning II [jet] fighter[,]" the Defense Department's most expensive weapons program.[90]

This episode, along with the Boeing breach discussed in Part I, helps illustrate some of the many facets of cybersecurity and challenges facing aerospace firms seeking to safeguard their trade secrets. Before turning to best practices in the next Part, though, it is first important to note that these efforts are not taking place in a legal vacuum. There is applicable U.S. law on point regulating the steps that companies, including those firms operating CI such as aerospace, must take to protect their assets and their customers' data. We review these laws, paying particular attention to the NIST Cybersecurity Framework, before moving on to discuss EU and international law. It is vital for business managers to have this comparative and international perspective since so many aerospace transactions involve multiple jurisdictions, with the United States and Europe remaining as important commercial hubs for the global space industry now valued at more than $300 billion.[91]

A. Applicable U.S. Laws to Mitigate Trade Secrets Theft

The problem presented by the theft of trade secrets has led some politicians and commentators to suggest that the United States needs a federal civil trade secret theft statute. As was mentioned in Part I, the current U.S. system utilizes only a federal criminal statute, the Economic Espionage Act (EEA) of 1996, and leaves civil actions to the states.[92] In 2012, as a response to growing concern over trade secrets theft, Congress enhanced the penalties for a violation of the EEA.[93] Yet this response is

---

89 *See* J. Nicholas Hoover, *NSA Chief: China Behind RSA Attacks*, INFO. WK. (Mar. 27, 2012), http://www.informationweek.com/government/security/nsa-chief-china-behind-rsa-attacks/232700341.

90 *See*, *e.g.*, Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009), http://online.wsj.com/article/SB124027491029837401.html; William Jackson, *RSA Confirms Its Tokens Used in Lockheed Hack*, GCN (June 7, 2011), http://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx. This passage was first published in the Preface of SHACKELFORD, *supra* note 18.

91 *See* Press Release, *Space Foundation's 2013 Report Reveals 6.7 Percent Growth in the Global Space Economy in 2012,* SPACE FOUND. (Apr. 2, 2013), http://www.spacefoundation.org/media/press-releases/space-foundations-2013-report-reveals-67-percent-growth-global-space-economy; ROBERT C. HARDING, SPACE POLICY IN DEVELOPING COUNTRIES: THE SEARCH FOR SECURITY AND DEVELOPMENT ON THE FINAL FRONTIER 2 (2012). In 2006, the satellite telecommunications' market alone exceeded $100 billion. *See* Keny Fuchter, *China's Military Space Strategy*, RAF AIR POWER REV. 53, 62 (2009).

92 *See infra* notes 54–56 and accompanying text.

93 The Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 18 U.S.C. § 1832(a) (2013); The Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 18 U.S.C. §§ 1831(a)-(b) (2013).

seen by many to be inadequate and there is speculation that a federal civil cause of action is pending.[94] The Obama Administration also conducted a further review of the existing legislation to determine if greater trade secret protections are warranted.[95]

Proposals for a federal civil cause of action have been a recurring theme in trade secret law for the past several decades.[96] Such advocates typically argue that the current system of disparate state laws creates inefficiencies and burdens interstate actors.[97] State courts also typically have less robust subpoena powers, weaker discovery, and more difficult jurisdictional hurdles to overcome. A federal cause of action would address these issues by establishing a uniform body of law and providing access to federal courts. Yet these arguments are not without their critics and the usefulness of a federal civil cause of action has been called into question.[98]

Despite these criticisms, several federal laws have recently been proposed to address the problem of trade secret theft. Take, for instance, the proposal by Representative Zoe Lofgren (D. California), who suggests that we should simply add a sentence to the EEA allowing any person injured by the theft of trade secrets to maintain a cause of action in federal court.[99] Or, consider the Trade Secret Protection Act of 2014, proposed by Representative Holding (R. N. Carolina).[100] This legislation is, as of this writing, before the House and Senate and provides a similar private cause of action for damages resulting from the misappropriation of trade secrets, as well as injunctive relief.[101] In both cases, the bills provide broad protection against the misappropriation of trade secrets and include in the definition of misappropriation "espionage through electronic or other means."[102] This language appears to be specifically targeted at the problem of cyber espionage. However, the likelihood of either bill being passed in the current partisan environment remains in doubt (estimates from govtrack.us as of September 2014 are one percent for the first bill, H.R. 2466, and thirty-

---

94 *See, e.g.*, Mark L. Krotoski, *The Time Is Ripe for New Federal Civil Trade Secret Law*, BNA (Dec. 3, 2014), http://www.bna.com/time-ripe-new-n17179917951/.

95 OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 12 (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_ strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

96 *See* Krotoski, *supra* note 94.

97 *See*, *e.g.*, Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 442 (1995).

98 *See* Argento, *supra* note 47.

99 PRIVATE RIGHT OF ACTION AGAINST THEFT OF TRADE SECRETS ACT OF 2013, H.R. No. 113-2466 (2013).

100 TRADE SECRET PROTECTION ACT OF 2014, H.R. 114-5233 (2014).

101 *See, e.g.*, *Will Congress Enact a Federal Trade Secrets Act in 2015?*, NAT'L L. REV. (Jan. 27, 2015), http://www.natlawreview.com/article/will-congress-enact-federal-trade-secrets-act-2015.

102 TRADE SECRET PROTECTION ACT OF 2014, H.R. 114-5233, at 11 (2014).

seven percent for the second, H.R. 5233).[103]

The applicability of the legislation to the cybercrimes at issue does not seem to be in question, yet these proposed domestic legislative acts do not address the overarching challenges posed by cybercrime: the hurdles of jurisdiction, international extradition, attribution, and prosecution. The chief problem in the enforcement of trade secret theft is that the assailants are able to engage in their unlawful activity from safe havens: countries that are either unwilling or unable to police their networks. U.S. statutes by themselves do relatively little to improve the ability of the United States to extradite criminals from countries that actively support the use of electronic means to steal trade secrets (the applicable international law is discussed below). And improving the ability to litigate trade secret misappropriation does not address the problems of cyber vulnerability that facilitates the ease of these thefts. This is not to suggest that the proposed legislation would be without merit. The misappropriation of trade secrets by those within the jurisdictional bounds of the United States would arguably be simplified, including the possibility of victims being able to seek treble damages for when the misappropriation is willful.[104] But these are only marginal benefits, and do not address the root concerns that generated the impetus for the legislation in the first place.

An example of U.S. legislation that could be more on point is the Chinese Communist Economic Espionage Sanctions Act.[105] This Act would go so far as to condemn the People's Republic of China and the Chinese Communist Party outright for the theft of U.S. trade secrets, and impose sanctions on "Chinese state-owned enterprises . . . for benefitting from cyber and economic espionage against the United States."[106] These actions would involve the seizure of assets belonging to persons associated with Chinese state-owned enterprises that come within the territorial jurisdiction of the United States, the denial of visas to Chinese nationals having ties to those Chinese state-owned enterprises, and the freezing of their assets held by financial institutions based in the United States.[107] However, while it may indeed be true that China is the main culprit targeting U.S. trade secrets and aerospace firms in particular, it is also a convenient scapegoat. Chinese networks are also vulnerable, by some estimates even more so than the United States,[108] and it is a simple matter to spoof IP addresses to fool

---

103 *See* GovTrack.us: Tracking the U.S Congress, https://www.govtrack.us/ (last visited Oct. 7, 2014).

104 TRADE SECRET PROTECTION ACT OF 2014, *supra* note 100, at 9.

105 Chinese Communist Economic Espionage Sanctions Act, H.R. 5103, 114th Cong. (2014).

106 *See id.* at 1.

107 *See id*. at 8–9.

108 *See China's Infrastructure Vulnerable to Cyber Attack*, FOXNEWS.COM (June 17, 2011), http:/

investigators as to the true source of an attack, as the Boeing case study from Part I illustrated. Instead of targeting politically convenient culprits, it may be a better use of legislative bandwidth to build on the momentum begun with the NIST Cybersecurity Framework with expanded information sharing provisions and incentive programs for firms to employ best-in-class cybersecurity.

Although the prospect of comprehensive cybersecurity regulation is unlikely, the Obama Administration has utilized executive action to strengthen U.S. cybersecurity by partnering with industry through the NIST Cybersecurity Framework process. In February 2014, NIST released its Framework for Improving Critical Infrastructure Cybersecurity, per Executive Order 13636.[109] The Framework is comprised partly of private-sector best practices that companies can adopt to better secure CI,[110] and includes criterion by which to determine cyber-risk and protocols to assist in mitigating those risks. Although the Framework does not create any binding obligations for private sector actors and has no means of enforcement for those that choose to adopt it, its uptake may well be establishing a cybersecurity standard of care in the United States even without Congressional action.[111] This holds the potential to spill over beyond traditional CI sectors to the private sector at large.

The Framework's basic structure divides cybersecurity into five broad "functions": identify, protect, detect, respond, and recover.[112] Each of these five functions is subdivided into categories, and each category contains subcategories paired with informative references.[113] The Framework uses these functions to establish four implementation tiers, which identify incremental levels of preparation and response that serve as guidelines for businesses to model their own practices based on their perceived needs.[114] Perhaps most importantly, the Framework provides a series of steps for

---

/www.foxnews.com/tech/2011/06/17/chinas-infrastructure-vulnerable-to-cyber attack/.

109 *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

110 Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

111 *See, e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as De Facto Mandatory*, HOMELAND SEC. NEWS WIRE (Mar. 4, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

112 NIST CYBERSECURITY FRAMEWORK, *supra* note 7, at 7.

113 *Id.* at 1.

114 *Id.*

organizations to follow to utilize the Framework to assess and address their current cyber risk exposure. This equips companies with a clearly articulated process to follow to begin improving their cybersecurity, including the identification of gaps. Rather than imposing strict governmental regulations that may be overly burdensome or incomprehensibly vague, the Framework allows companies to incorporate cyber risk management in a manner that is consistent with their business goals and financial capabilities. By establishing clear guidelines for private-sector actors, the NIST Framework promotes flexible cybersecurity standards and may well serve to facilitate the protection of trade secrets both in the United States and in other jurisdictions.

B. EU Cybersecurity Initiatives Related to Trade Secrets Theft

The European Union's approach to securing CI has been motivated by the March 2014 Madrid terrorist bombings.[115] In the aftermath of the attacks, the EU Commission—the executive body of the European Union—adopted suggestions for how to enhance "prevention, preparedness and response to terrorist attacks involving [CI]."[116] CI in the European Union is defined broadly, referring to infrastructure that is "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being, and the destruction or disruption of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[117] Examples include sectors similar to those often cited in the United States, such as "telecommunication and energy networks, financial services and transport systems, health services, and the provision of safe drinking water and food."[118] However, there is some question as to whether aerospace falls under this rubric. It is not singled out in applicable EU directives discussing critical infrastructure, though related areas are such as communications, government, and transport.[119] Thus, it would be prudent for managers to treat aerospace as falling under these regulations,

---

115 *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 153 (2014) (opining that critical Infrastructure, as used in the EU context, demonstrates the extent to which securing infrastructure is a regional, and not solely national, issue. The term CI, though, suffers from many of the same ambiguities as CNI.)

116 *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, at 2, COM (2006) 786 Final (Dec. 12, 2006) [hereinafter *Communication Concerning EPCIP*].

117 *Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)*, at 10, COM (2008) 676 Final (Oct. 27, 2008).

118 *Id.* at 2.

119 *Critical Infrastructure Protection*, EUROPA, (Aug. 17, 2010), http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.

especially the more expansive set discussed next.

Neither cyber offence nor cyber defense stops at national borders, especially in regions as economically integrated as Europe.[120] As a result, in February 2013, the Communication on Critical Information Infrastructure Protection committee introduced a proposed cybersecurity directive that dramatically changed the status quo of regulatory efforts and even went several steps further than the analogous U.S. efforts, such as the NIST Framework. In particular, if implemented, the EU policy would require firms to meet EU-developed standards, which could mean that these companies may "fundamentally have to change the way [their] business operates."[121] Among much else, this regime would require many firms with some nexus to the Internet to invest in new technologies, develop procedures to prove compliance to national and EU regulators, and undertake enhanced cyber risk mitigation measures to better manage attacks.[122] Aerospace firms would likely be covered by these regulations and would then be faced with a choice of whether to develop a unique set of cybersecurity best practices to cover their European operations or simply adopt these standards in their global operations; thus, these aerospace firms would be assured of regulatory compliance but at increased cost. Firms in the U.S. context must often undertake a similar analysis when deciding whether to comply with oftentimes more stringent California regulatory requirements solely for that market or adopt them more broadly across their national operations making California laws at times de facto national regulations. It is also worth noting that EU regulators have reportedly had

---

120 *See Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*, at 3, COM (2013) 48 Final (Feb. 7, 2013).

121 Warwick Ashford, *How Will EU Cyber Security Directive Affect Business?*, COMPUTER WKL'Y (Feb. 19, 2013), http://www.computerweekly.com/news/2240178256/How-will-EU-cyber security-directive-affect-business (citing Stewart Room, a partner at Field Fisher Waterhouse, who argues that this directive will mean that other firms beyond telecom companies will face regulatory burdens related to cybersecurity, including e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services, app stores).

122 *Id.*; *see also Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR. COMM'N, at 2–6 (Feb. 7, 2013) (Espousing an Internet freedom agenda that includes universal access, democratic and "efficient multi-stakeholder governance," and a focus on attaining "cyber resilience." To achieve this, the directive sets out a number of goals, including setting national-level cybersecurity standards, creating national and regional CERTs, sharing private-sector best practices, and regularly assessing cyber risk—especially for firms operating critical infrastructure—so as to build a "cybersecurity culture."). *But see* Stephen Gardner, *Member States Reportedly Unconvinced on Need for EU Cybersecurity Directive*, BLOOMBERG BNA (June 3, 2013), http://www.bna.com/ member-states-reportedly-n17179874317/ (reporting on questions from ministers arising from this mandate approach and noting that "other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard to cybersecurity standards" such as the NIST framework and worrying about creating "inconsistencies for companies whose operations span several jurisdictions.").

regular contact with NIST officials over the extension of the NIST Cybersecurity Framework to Europe. Other nations, including Japan, India, and the Republic of Korea, have also been active in NIST-sponsored cybersecurity deliberations.[123]

C. The Role of International Law

No nation is an island in cyberspace, and as such, international law also has a vital role to play in enhancing cybersecurity and protecting trade secrets. Among the best-known and most important international treaties regulating cybersecurity is the Council of Europe's Convention on Cybercrime, popularly known as the Budapest Convention.[124] Myriad criminal offenses are defined under the Budapest Convention, including: illegal access, illegal interception, data interference, system interference, and misuse of devices.[125] The Convention calls on signatories to adopt domestic laws to criminalize these offenses and to establish a regime to enhance international cooperation. As of October 2014, forty-three nations had ratified the accord.[126] However, protections of trade secrets are not spelled out in the agreement, and enforcement mechanisms for noncompliance remain absent.[127] Thus, while the Budapest Convention remains something of a gold standard for international collaboration to manage cyber attacks, its utility to the aerospace sector generally and the cause of trade secrets protections in particular is questionable.

Aside from dedicated cybersecurity treaties, there is a range of applicable international law, both above and below the armed attack threshold, which defines when the law of war is activated.[128] In the trade secrets context, though, among the most applicable laws are investment and

---

123 *Update on the Cybersecurity Framework*, NIST 4 (July 31, 2014), http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf ("NIST and other U.S. government officials have had discussions about the Framework with multiple foreign governments and regional representatives including organizations throughout the world, including—but not limited to—the United Kingdom (UK), Japan, Korea, Estonia, Israel, Germany, and Australia.").

124 *Convention on Cybercrime*, COUNCIL OF EUROPE (Nov. 23, 2001), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; *see also* MARCO GERCKE, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL OPTIONS 127–28 (INT'L TELECOMM. UNION, 2012), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (listing other relevant model laws, including the Commonwealth Model Law on Computer and Computer-related Crime).

125 Budapest Convention, arts. 2–6.

126 *See Convention on Cybercrime*, COUNCIL OF EUR. TREATY OFF., http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/06/2013&CL=ENG (last updated Feb. 3, 2014).

127 *See id.*

128 *See generally* Chapter 6 in SHACKELFORD, *supra* note 18.

trade treaties.[129] Bilateral investment treaties (BITs) have long been an important component of international investment law.[130] By 2013, there were nearly 3,000 BITs involving the vast majority of countries.[131] These agreements cover a huge range of industry sectors and business activities and generally include a forum for resolving disputes in the form of investor-state arbitration.[132] At the July 2013 U.S.—China Strategic and Economic Dialogue, the United States and China publicized plans to begin negotiating an expansive BIT that will reportedly include the difficult issue of enhancing bilateral cybersecurity.[133] According to U.S. Treasury Secretary Jacob J. Lew, if successful, this would be "the first time China has agreed to negotiate a bilateral investment treaty, to include all sectors and stages of investment, with another country."[134] Although still mostly hypothetical,[135] these agreements, including the proposed U.S.-China BIT, could pave the way for U.S. aerospace companies to file claims alleging trade secrets theft against foreign companies and perhaps even governments and have their case heard before a panel of neutral arbitrators.[136] Although there would remain a question of whether a foreign sovereign would abide by a negative ruling, this state of affairs would likely be preferable to the current dearth of legal options for affected companies seeking to bring cases alleging trade secrets theft either in U.S. or foreign courts.

Aside from BITs, cybersecurity is also becoming an important topic in regional and global trade negotiations. Ongoing U.S.–European Union trade talks have been shaped at least initially by concerns over NSA surveillance

---

129 *See* Shackelford et al., *supra* note 57.

130 *See, e.g.*, UNITED NATIONS CONF. ON TRADE & DEV. (UNCTAD), BILATERAL INVESTMENT TREATIES 1995-2006: TRENDS IN INVESTMENT RULEMAKING xi (2007), http://unctad.org/en/Docs/iteiia20065_en.pdf.

131 UNCTAD, WORLD INVESTMENT REPORT 2013: GLOBAL VALUE CHAINS: INVESTMENT AND TRADE FOR DEVELOPMENT 101 (2013), http://unctad.org/en/PublicationsLibrary/wir2013_en.pdf. There were also another 339 trade agreements, bringing the total number of international investment agreements to 3,196. *Id.*; *see also* ICSID Database of Bilateral Investment Treaties, ICSID, https://icsid.worldbank.org/ICSID/FrontServlet?requestType=ICSIDPublicationsRH&actionVal=ViewBilateral&reqFrom=Main (last visited Apr. 29, 2014).

132 *See* Gus Van Harten, INVESTMENT TREATY ARBITRATION AND PUBLIC LAW 6 (2007).

133 *See* Annie Lowrey, *U.S. and China to Discuss Investment Treaty, but Cybersecurity Is a Concern*, N.Y. TIMES, July 12, 2013, at A5.

134 *Id.* (internal quotations omitted).

135 *Cf.* Leslie A. Pappas, *Speed Up Bilateral Treaty Negotiations and Build Trust, China's Xi Jinping Says*, 31 INT'L TRADE REP. 1685 (2014) (noting pressure from China to hasten U.S.-China BIT negotiations).

136 *See Xi Calls for More Strategic Trust Between China, U.S.*, XINHANET (Sept. 9, 2014), http://news.xinhuanet.com/english/china/2014-09/09/c_126968104.htm ("Xi also urged the two sides to speed up negotiations of a bilateral investment treaty, cement military-to-military ties, strengthen communication and coordination on climate change, fighting against terrorism, and regional and global flash points.").

programs and intellectual property protections.[137] The proposed Trans-Pacific Partnership also has a cybersecurity component,[138] and even the World Trade Organization (WTO) employs enforcement mechanisms that may be applicable to cyber attacks if national security concerns could be overcome.[139] Together, these investment and trade regimes could provide a basis for fostering bilateral and regional collaboration to enhance global cybersecurity generally and better protect trade secrets in particular at a time of slow progress on domestic and multilateral progress toward cybersecurity policymaking.[140] But they likely will not be enough absent the private sector taking proactive steps to improve cybersecurity from the ground up.

III. NEED FOR PROACTIVE CYBERSECURITY BEST PRACTICES IN THE AEROSPACE SECTOR

Imagine the feeling of excitement and opportunity that the Model T Ford represented to consumers in the early twentieth century. That newfound freedom came at a price, however, with early cars lacking safety features such as seatbelts, adjustable mirrors, and crumple zones to absorb impact, to say nothing of airbags. Despite the fact that many of these safety

---

137 *See, e.g.*, Doug Palmer, *U.S., EU Launch Free Trade Talks Despite Spying Concerns*, INS. J. (July 9, 2013), http://www.insurancejournal.com/news/international/2013/07/09/297817.htm. *But see* James Fontanella-Khan, *Brussels Opposes German Data Protection Push,* FIN. TIMES, Nov. 5, 2013, at 8 ("Brussels has ruled out a German push to include data protection rules in a proposed EU–U.S. free trade pact, arguing that it could derail the talks and ultimately weaken Europeans' rights to privacy.").

138 *See* Kevin Collier, *Sen. Ron Wyden on the Problems with the Trans-Pacific Partnership*, DAILY DOT (Sept. 19, 2012), http://www.dailydot.com/politics/ron-wyden-trans-pacific-partnership/.

139 However, regarding the latter, while the WTO has been used as a forum to air broader concerns among the Member States, it has to date been a factor in the cybersecurity context because of provisions allowing nations to shirk their free trade commitments when they conflict with national security. *See, e.g.,* ALLAN A. FRIEDMAN, BROOKINGS INST., CYBERSECURITY AND TRADE: NATIONAL POLICIES, GLOBAL AND LOCAL CONSEQUENCES 10–11 (2013), *available at* http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookings cybersecuritynew.pdf; Mark L. Movsesian, Essay, *Enforcement of WTO Rulings: An Interest Group Analysis*, 32 HOFSTRA L. REV. 1, 1–2 (2003) (describing the WTO Dispute Settlement Understanding and noting that trade disputes between nations "are to be resolved in adversarial proceedings before impartial panels of experts" under this system); James A. Lewis, CTR. STRATEGIC & INT'L STUD., Conflict and Negotiation in Cyberspace 49-51 (2013), *available at* https://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf (discussing the applicability of the WTO dispute resolution processes to help manage cyber espionage). This limitation in the WTO composition underscores the need for a bilateral and regional approaches to enhancing cybersecurity.

140 *See, e.g.*, Scott J. Shackelford, Essay, In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012, 64 STAN. L. REV. ONLINE 106 (2012), *available at* http://www.stanfordlawreview.org/online/cyber-peace; Tom Gjelten, *Seeing the Internet as an "Information Weapon,"* NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701 (discussing the fact that United Nations-sponsored cyber disarmament discussions have been ongoing since the late 1990s without much to show for it).

features seem intuitive in retrospect, it took some time to standardize them. Formal studies were needed to assess risk, and then stakeholders—including companies, consumers, and governments – needed to perceive risks as important and devote resources to implementing fixes. One of the first popular reports pushing improving car safety was published by *Popular Science* in 1950, featuring the attention-grabbing title, "Making the Death Seat Safer," and highlighting the potential of seatbelts and padded dashboards.[141] However, it was not until 1958 that a Volvo engineer invented the three-point lap and shoulder seatbelt.[142] It then took nearly two decades before the results of crash tests were published to inform consumers of cars' variable safety performances.[143] The first U.S. law mandating the use of seat belts was not passed until 1984.[144]

To continue this analogy we are now, unfortunately, in the 1960s with regards to cybersecurity. Regulations are present, but they have been slow to develop and do not reflect technological best practices. Nor is there widespread agreement on what the best ways are to mitigate cyber threats, or even on the scope of the problem; reaching consensus on what counts as an automobile accident is a far simpler proposition than defining a "cyber attack."[145] Still, some lessons may be gleaned from the morass of imperfect cyber attack data. Best practices are slowly arising, a process that may be hastened by the NIST Cybersecurity Framework process and the increasing attention being paid to cybersecurity by consumers and investors. Moreover, the importance of information sharing in the private sector and with policymakers is also now more widely accepted. We explore these developments next and conclude by couching them within a polycentric framework for promoting cyber peace.

A. Summary of Best Practices

As seen in the NASA case study, perhaps the simplest yet most important element to any effective cybersecurity strategy is an organizational structure that empowers cybersecurity personnel. Too often we hear the story of a major corporation that suffers a massive data breach, only to have it revealed that they did not employ a CISO or similar executive. To take one recent example, "like Sony before it, Target did not

---

141 *See* George H. Waltz, Jr., *Making the Death Seat Safer*, 157 POP. SCI. 82 (July 1950).

142 *See id.*

143 *See id.*

144 This passage first appeared in Chapter 5 of SHACKELFORD, *supra* note 18. Special thanks go to Amanda N. Craig for her help with this research.

145 NAT'L RES. COUNCIL OF THE NAT'L ACADS., TECH., POLICY, LAW, & ETHICS REGARDING U. S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens et al. eds., 2009).

have a" CISO prior to its late 2013 data breach.[146] Both firms do now.[147]

Although there are numerous names and positions that can adequately fill the role of a centralized cybersecurity officer, it is of upmost importance that cybersecurity be implemented within the C-suite structure. Security often represents a negative in the eyes of the corporate finances without clear positives given the lack of reliable data on cybersecurity cost-benefit analysis, and as such it is not always a popular topic to bring up. But by implementing cybersecurity within the C-suite, a firm can help assure itself that cybersecurity issues will be proactively considered prior to the occurrence of a breach, and that the company will have an accountable individual to turn to when vulnerability is exploited.

Yet it is not enough to simply acknowledge that cybersecurity is an issue; organizations must take proactive steps to mitigate and deter cyber threats if they are to be adequately prepared for future cyber threats. The most effective corporate cybersecurity policies are those that attempt to preempt cyber attacks, hiring white hat hackers to conduct regular penetration testing, and utilizing employee awareness campaigns to ensure that the cybersecurity strategy is widely distributed and understood.[148] Indeed, as the Boeing case study illustrated, firms must make education about cybersecurity issues a central part of the corporate learning process. Even the most advanced technical protections can often be undone if the employees of the company fail to utilize appropriate security measures. Simple lessons like not sharing or reusing passwords and identifying spam and phishing emails often have the most profound impact upon a company's security.[149] The good news is that more firms seem to be taking these lessons to heart. According to one 2010 survey, sixty-five percent of companies had "an overall information security strategy" in 2009, up from fifty-nine percent in 2008.[150] Yet in 2012, according to a PwC survey, just forty-three percent of organizations with strategies called those strategies: 1) "effective," and 2) themselves "proactive" at implementing their plans,[151] including the establishment of robust information sharing to protect against

---

146 *See* Fred Donovan, *Target Did Not Have CISO to Oversee Information Security Prior to Massive Breach*, FIERCE SEC. (Mar. 10, 2014), http://www.fierceitsecurity.com/story/target-did-not-have-ciso-oversee-information-security-prior-massive-breach/2014-03-10.

147 *See id.*

148 *See generally* SHACKELFORD, *supra* note 18, at Chapter 5.

149 *See generally id*. (providing a more comprehensive summary of corporate cybersecurity best practices in Chapter 5).

150 *Trial by Fire: What Global Executives Expect of Information Security*, PWC 18–19 (Oct. 2009), http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf.

151 *Eye of the Storm: Key Findings from the 2012 Global State of Information Security Survey*, PwC 6 (2012), http://www.pwc.co.nz/global-state-of-information-survey.aspx.

known cyber threats.[152] We can do better.

B. The Case for an Aerospace Information Sharing Organization

Information Sharing Analysis Centers (ISACs) were first established in 1998 as a response to Presidential Decision Directive 63, which called specifically for a public-private partnership to reduce vulnerability to cyber threats to CI.[153] This was extended in 2003 under the Patriot Act, and has resulted in the creation of ISACs for numerous CI sectors.[154] ISACs are private sector, non-profit organizations that serve as centralized hubs for the sharing of information related to cybersecurity threats.[155] Through ISACs, companies with similar cyber-risk exposure can anonymously communicate cyber attacks perpetrated against them, allowing for rapid analysis, response, and vulnerability sharing to other members of the group.[156] ISACs essentially serve as a repository for vulnerability information, which is useful in compiling the risks, providing advice in real time, and communicating information to other ISAC members.[157] Through information sharing, organizations can help immunize themselves from the threats encountered by others, including, we argue, aerospace organizations.

Perhaps the most fundamental attribute of successful ISACs is anonymization. ISACs often (and indeed should) include government intelligence and law enforcement agencies within their ranks, both as repositories of threat information and as analytical powerhouses to pursue perpetrators.[158] But the inclusion of government agencies in data sharing arrangements would necessarily arouse the fear and suspicion of private-sector actors, especially in the post-Snowden world where the specter of government regulation or enforcement may overshadow their interest in proactive threat resolution, and especially among tech firms. Furthermore, attribution, even among private-sector members, may influence business dealings as a company that is repeatedly subjected to cyber attacks may be deemed to be a less desirable business partner. By ensuring that the data submitted to an ISAC is anonymized prior to sharing, private actors are enticed to share information without fear of public or private repercussions

---

152 *Id.*

153 Presidential Decision Directive 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

154 Electricity Sector Information Sharing and Analysis Center, ES-ISAC, http://www.esisac.com/SitePages/Home.aspx (last visited Oct. 1, 2014).

155 *Id.*

156 NAT'L COUNCIL OF ISACS, http://www.natlisacs.org (last visited October 1, 2014).

157 *See id.*

158 *See Cybersecurity Results*, DHS, http://www.dhs.gov/cybersecurity-results (last visited Oct. 17, 2014).

(that is, unless of course the repository itself is breached).

The use of anonymization, however, should not be interpreted as a strict requirement for all ISAC submissions. Rather, successful ISACs utilize a tiered information sharing system, where data sharing may be restricted or conditioned based upon the nature of the information at issue. An example system is the "traffic light protocol" (TLP) utilized by the Financial Sector ISAC (FS-ISAC).[159] This allows companies that submit data to the FS-ISAC to designate the degree of information sharing with a color: red for strict, or named party only, distribution; amber for limited distribution within their own organization; green for full distribution within the ISAC community, and white for full public distribution.[160] Therefore, companies can choose to make submissions that are either anonymous or attributed and can exercise greater control over who will learn of their connection to the submission. Through the use of tiered systems for information sharing, companies are given greater control over the extent that their data is attributable to them, while still facilitating the maximum agreeable data distribution.

Furthermore, as alluded to previously, the inclusion of government agencies is essential to optimal functioning in response to cyber threats. Government agencies like the NSA, FBI, and DHS all bring vast technological prowess, experience in cyber response processes, and data regarding vulnerabilities and best practices.[161] Indeed, the initial PDD that led to the establishment of ISACs called for such "public-private partnership to reduce vulnerability."[162] From the outset, ISACs have been designed with the intention of allowing greater information sharing between public and private actors, and ISACs must utilize the resources offered by these government agencies if they are to most effectively minimize vulnerabilities in their sector. However, this information sharing should be a two-way street with the public sector similarly learning from business, along with businesses, including aerospace firms, learning from one another.

ISACs should also consider other ISACs as resources when analyzing and responding to cyber threats. Although each industry sector faces unique challenges, many of the concerns overlap sectors, and utilizing the expertise

---

159 *See* FINANCIAL SERVICES INFORMATION SHARING & ANALYSIS CENTER OPERATING RULES 18 (FS-ISAC), http://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2012.pdf.

160 *Traffic Light Protocol Matrix and Frequently Asked Questions*, US-CERT, https://www.us-cert.gov/tlp (last visited Oct. 8, 2014); *see also* Denise Anderson, *The Role of the ISACs in Critical Infrastructure Resilience,* RSA CONF., http://www.rsaconference.com/writable/presentations/file_upload/cle-t10-the-role-of-the-isacs-in-critical-infrastructure-resilience.pdf (last visited Oct. 8, 2014).

161 *See Cybersecurity Results*, supra note 158.

162 Presidential Decision Directive, *supra* note 153.

and experience of other ISACs prevents any one industry from being secluded from developments in cybersecurity best practices. As other repositories of information sharing with similar priorities and operating structures, ISACs must learn from one another to optimize cyber threat response, especially for organizations that straddle critical infrastructure designations like aerospace.

Focusing on the aerospace context, lessons may be taken from the Financial Services ISAC (FS-ISAC) and National Health ISAC (NH-ISAC) among others in crafting an aerospace information-sharing organization, which would represent an expansion of the aviation ISAC currently in development of which Boeing is a founding member.[163] FS-ISAC provides useful experience as both a high-volume target of cyber attackers, as well as an industry with significant government oversight. Like aerospace and the FAA, the financial services sector has learned how to incorporate SEC, DHS, CDC, and other governmental oversight into its information sharing structure.[164] Similarly, NH-ISAC would provide useful experience as a sector that is increasingly focused on the protection of trade secrets against theft and misappropriation. Like aerospace, many elements of the health sector rely on trade secrets for the protection of intellectual property rights,[165] and this focus on trade secrets has led to the crafting of information sharing practices that attempt to prevent the over-disclosure of this confidential information.[166]

Yet other criteria are also vital indices of a successful ISAC. Tools like tiered memberships, open source databases, cyber threat drills and National Level Exercises, as well as other cybersecurity trends should be considered to optimize information sharing and ensure preparedness for cyber threats in the aerospace context. Additionally, improving the means of information sharing is also increasingly important, as the sheer volume of information shared may be overwhelming and thus unhelpful. Tools such as wikis, web portals, and digests may be preferable to the traditional listserv, as these allow for better organization of the flow of data.[167] These platforms

---

163 *See Securing Airline Information on the Ground and in the Air*, BOEING, http://www.boeing.com/commercial/aeromagazine/articles/2012_q3/5/ (last visited Oct. 19, 2014).

164 *See* Cybersecurity: Hearing Before the House Energy and Commerce Committee, 113th Cong. 4-6 (2013) (testimony of Charles Blauner, on behalf of the American Bankers Association), a*vailable at* http://www.fsscc.org/fsscc/legislative/2013/Cybersecurity-May21-Final.pdf.

165 Gibbons et al., *The Increasing Importance of Trade Secret Protection in the Biotechnology, Pharmaceutical and Medical Device Fields*, 89 J. Pat. & Trademark Off. Soc'y 261, 262-264 (2007).

166 Memorandum of Understanding Between the Nat'l Health Info. Sharing & Analysis Ctr., Inc. and the U.S. Food and Drug Admin. Ctr. for Devices and Radiological Health (Aug. 26, 2014), *available at* http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/OtherMOUs/ucm412565.htm.

167 Tay Pei Lyn Grace, *Wikis as a Knowledge Management Tool*, J. KNOWL. MGMT., Oct. 2009,

emphasize searching, tagging, and categorizing threats, ensuring that users can query based on meaningful metrics.[168] But as technologies improve and cybersecurity norms evolve, so too must ISACs update their practices to reflect this changing world.

Critical infrastructure is not the only context in which cyber threat information sharing is taking off; indeed, it is becoming commonplace in retail and other commercial sectors. Recently, the Retail Industry Leaders Association (RILA) launched the Research Cyber Intelligence Sharing Center (R-CISC), which has at its center a Retail ISAC.[169] The retail sector has been increasingly under fire during the past several years for its repeated security breaches resulting in the theft of customer data.[170] Incidents like the Target breach of 2013[171] and the Home Depot breach from 2014[172] received major public scrutiny and prompted systemic changes, both in the structure of the companies targeted[173] and in the retail sector generally. The R-CISC is part of an industry wide response that acknowledges the growing problem of cyber attacks and attempts to improve cybersecurity through information sharing and public/private partnerships.[174] This development helps to demonstrate the increasing perceived importance of expanding information sharing networks across an array of industries and sectors.

For the aerospace sector in particular, information sharing would serve as a powerful resource in the management of cyber threats. Information sharing is already becoming a mainstay in the commercial aviation sector. In 2006, President Bush issued Homeland Security Presidential Directive 16, established a National Strategy for Aviation Security, and led to the creation of the Air Domain Intelligence Integration Center (ADIIC), which is a centralized hub for government information on aviation security information.[175] This was furthered in 2014 with the announcement of an Aviation ISAC (Aero-ISAC) that would coordinate with the ADIIC to

---

at 64.

168 *Id.*

169 R-CISC: Retail Cyber Intelligence Sharing Center, RILA, *available at* http://www.rila.org/rcisc/Home/Pages/default.aspx

170 *See, e.g.*, *Data Breach* FAQs, TARGET, *available at* https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ (last visited Oct. 20, 2014).

171 *See id.*

172 Maggie McGrath, *Home Depot Confirms Data Breach, Investigating Transactions from April Onward,* FORBES (Sept. 8, 2014), http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/.

173 Anna Prior, *Target Hires Tech-Security Chief from GM,* WALL ST. J. (June 10, 2014), http://online.wsj.com/articles/target-hires-information-security-chief-1402422451.

174 *See* R-CISC, *supra* note 169.

175 Homeland Security Presidential Directive 16 (June 22, 2006), *available at* http://fas.org/irp/offdocs/nspd/nspd-47.pdf.

facilitate public/private information sharing.[176] Yet this endeavor has unnecessarily limited its own scope, and the information sharing would benefit from broadening to include aerospace within its ambit.

The inclusion of aerospace writ large in the proposed Aero-ISAC is a natural extension of this industry to cover related threats, especially to valuable trade secrets. Aerospace and aviation naturally have a great deal of overlap, which suggests that aerospace would be functionally included to some degree even if not designed as such. The inclusion of aerospace would also broaden the scope of the organization, bringing in major actors like NASA and SpaceX, whose experiences might otherwise be isolated. Furthermore, the attackers that are interested in aviation technologies are likely just as interested in aerospace technologies, and this overlap of attackers would suggest that the data from individual attacks is relevant across both sectors. Given the overlap in technical problems, member firms, and cyber threats, expansion of the Aero-ISAC to an aerospace ISAC is a logical and beneficial step.

The Aero-ISAC should be implemented to incorporate those elements that have best served other sector ISACs. This would include anonymized reports, tiered information sharing, and partnerships with other ISACs and information sharing agencies such as ADIIC. A successful Aero-ISAC would also likely include a tiered governance structure in which larger corporations would purchase premium memberships that ensure high-level, decision-making authority, recognizing both their influence in field and the scope of their resources. This means that the Aero-ISAC would be a partnership of a large number of aerospace firms, but that the central governing body would be composed of major market actors, with the daily operations being independently controlled. However, in this structure, minority representation for smaller aerospace firms would also be vital since they are perhaps even more concerned with safeguarding trade secrets, the lifeblood of many startups. And finally, the Aero-ISAC would reach out to governmental agencies like the DHS and FAA, as well as to international cyber threat repositories such as the International Multilateral Partnership Against Cyber Threats (IMPACT)[177] to ensure the maximum of information sharing and analytics. By increasing the interconnectivity throughout the sector, the Aero-ISAC can maintain private-sector

---

176 Rachel King, *Aviation Industry and Government to Share Cyber Threats in New Intelligence Center*, WALL ST. J. (Apr. 15, 2014), http://blogs.wsj.com/cio/2014/04/15/aviation-industry-and-government-to-share-cyberthreats-in-new-intelligence-center.

177 *About Us*, IMPACT, http://www.impact-alliance.org/aboutus/ITU-IMPACT.html (last visited Feb. 9, 2014); *see Strategy*, ITU, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Strategy.aspx (last visited Jan. 24, 2014); IMPACT, http://www.impact-alliance.org/aboutus/mission-&-vision.html (last visited Jan. 24, 2014).

independence while facilitating cybersecurity. The Obama Administration's cybersecurity information sharing proposals could help in this regard to break down the siloed approach to managing the cyber threat and allowing best practices to diffuse more readily between critical infrastructure sectors and with the broader economy.[178]

In many respects the biggest hurdle in cybersecurity is keeping pace with the rapidly evolving nature of the threat. This observation applies doubly for the aerospace sector; the shear scope of data that must be protected means that it is subject to novel attacks frequently, while the subject matter's demand makes it a prime target for both international criminal groups and governments alike. The large footprint of defense contractors like Boeing and Lockheed Martin means that they each possess huge repositories of data on cyber threats, and a purely isolationist view to security weakens both themselves and the industry as a whole, thus illustrating the need for a polycentric approach to enhancing aerospace cybersecurity.

C. Necessity for a Polycentric Approach

Professor Elinor Ostrom and her collaborates deserve credit for developing the field of polycentric governance as part of her work on collective action problems.[179] The basic notion of polycentric governance, as applied to global collective action problems such as cyber attacks, is the argument that "a single governmental unit" may be incapable of fostering cyber peace in part because free riders discourage "trust and reciprocity" between stakeholders.[180] Some stakeholders enjoy the benefits of others' sacrifices without realizing the costs; solutions "negotiated at the global level, if not backed by a variety of efforts at national, regional, and local levels, are not guaranteed to work well."[181] Professor Ostrom thus

---

178 *See* White House Press Release, SECURING CYBERSPACE—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

179 *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 10 (World Bank, Policy Research Working Paper No. 5095, 2009), *available at* http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.;

179 *Id.* at 35; *see* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* at 9 (Harv. Proj. on Int'l Climate Agreements, Discussion Paper No. 33, 2010) (published as 9 PERSP. ON POL. 7 (2011)) (discussing the feasibility of managing diverse problems within the climate change context with diverse institutions).

180 *Id.* at 35; *see* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* at 9 (Harv. Proj. on Int'l Climate Agreements Discussion Paper No. 33, 2010) (published as 9 PERSP. ON POL. 7 (2011)) (discussing the feasibility of managing diverse problems within the climate change context with diverse institutions).

181 Ostrom, *supra* note 179, at 4.

challenged the theory of collective action,[182] arguing that instead of top-down, state-imposed regulations, researchers found that small groups across an array of contexts do in fact cooperate and can create the proper incentives and conditions for optimal collective action.[183] The polycentric regimes were more flexible and benefited from local knowledge, unlike top-down regulatory schemes.[184] These observations corroborated experiments finding that externally imposed regulations can in fact crowd out individuals' voluntary cooperative behavior.[185] An inflexible, comprehensive regime then could actually stifle innovation by crowding out smaller-scale efforts might be more effective at promoting, for example, cyber peace.[186] That is in part why Professor Ostrom has argued that polycentric regulation is "the best way to address transboundary problems . . . since the complexity of these problems lends itself well to many small, issue-specific units working autonomously as part of a network that is addressing collective action problems. It is an application of the maxim, 'think globally, but act locally.'"[187] Bottom-up information sharing efforts such as those described above in the aviation and retail sectors, along with collaborative policymaking efforts such as the NIST Cybersecurity Framework that helps to identify and instill best practices, are examples of such a polycentric undertaking to promote cybersecurity. Similar private-sector led endeavors such as private-sector certification schemes identifying aerospace companies with the most secure supply chains should receive continuing encouragement to refine cybersecurity best practices most applicable to the aerospace sector as part of an ongoing

---

182 The traditional theory of the collective action problem was first articulated in the 1960s Mancur Olsen, an economist and social scientist from the University of Maryland. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (providing the first comprehensive explication of the collective action problem).

183 *See* Ostrom, *supra* note 179, at 8-10 (discussing he shortcomings of the conventional theory of collective action); Elinor Ostrom, Public Entrepreneurship: A Case Study in Ground Water Basin Management (1965) (unpublished Ph.D. dissertation, Univ. of Calif.); IMPROVING IRRIGATION GOVERNANCE AND MANAGEMENT IN NEPAL (Ganesh Shivakoti & Elinor Ostrom, eds., 2002); Elinor Ostrom & Harini Nagendra, *Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory*, 103 PROC. NAT'L ACAD. SCI. 19224, 19224-25 (2006).

184 *See id.*

185 *See* Bruno S. Frey & Felix Oberholzer-Gee, *The Cost of Price Incentives: An Empirical Analysis of Motivation Crowding-Out*, 87 AM. ECON. REV. 746 (1999); Ostrom, *infra* note 186, at 656 (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAVIOR & ORG. 273 (2008) (finding "externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate.").

186 *See, e.g.*, Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010).

187 Interview with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, in Bloomington, Ind. (Oct. 13, 2010). This research builds from Scott J. Shackelford, Timothy L. Fort, & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 UNIV. PENN. J. INT'L L. 353 (2015).

polycentric effort at safeguarding trade secrets and promoting cyber peace.

CONCLUSION

This Article has surveyed the multifaceted cyber threat facing the private sector and has argued for the necessity of a polycentric response recognizing in particular the vital role of information sharing and implementation of the NIST Cybersecurity Framework to help stem the theft of valuable trade secrets. The aerospace sector is in some ways unique in that it is dominated by relatively few actors, which in some ways makes the task of information sharing easier if economic, political, and security concerns may be overcome. The fact that this process has begun with the proposed Aviation ISAC is encouraging, but these efforts should be expanded to the aerospace sector writ large and infused with best practices gleaned from other successful ISACs discussed in Part III. As firms of all sizes and across myriad sectors work to better manage cyber attacks, aerospace has the opportunity to become a norm entrepreneur leading the way both above and beneath the clouds to a new frontier complete with some measure of cyber peace. It is an ambitious mission that, perhaps, these organizations are in some ways well situated to undertake if information-sharing barriers may be overcome and proactive cybersecurity measures encouraged.