Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things

LAWRENCE J. TRAUTMAN* & PETER C. ORMEROD**

Cyber breaches continue at an alarming pace with new vulnerability warnings an almost daily occurrence. Discovery of the industrial virus Stuxnet during 2010 introduced a global threat of malware focused toward disruption of industrial control devices. By the year 2020, it is estimated that over 30 billion Internet of Things (IoT) devices will exist. The IoT global market spend is estimated to grow from $591.7 billion in 2014 to $1.3 trillion in 2019 with a compound annual growth rate of 17%. The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019. With this tremendous growth in both data and devices, a security nightmare appears more reasonable than not. The proliferation of novel consumer devices and increased Internet-dependent business and government data systems introduces vulnerabilities of unprecedented magnitude. This paper adds to our understanding of the development of cyber vulnerabilities resulting directly from: (1) the Stuxnet code and its progeny, and (2) widespread malware exposure associated with the IoT.

* B.A., The American University; M.B.A., The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Assistant Professor of Business Law and Ethics at Western Carolina University. He may be contacted at Lawrence.J.Trautman@gmail.com.

** B.A. (magna cum laude), J.D., The George Washington University Law School. Mr. Ormerod is an adjunct professor at Western Carolina University. He may be contacted at ormerod.peter@gmail.com.

I. INTRODUCTION

Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years.

Daniel R. Coats
Director of National Intelligence
May 11, 2017[1]

Cyber breaches continue at an alarming pace and new vulnerability warnings are an almost daily occurrence.[2] The following categories of U.S. infrastructure have been identified as critical to the well-being of the nation: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil, and gas production; and storage.[3] Discovery of the industrial virus Stuxnet during 2010 introduced a global threat of malware that targets and destroys industrial control devices.[4]

---

[1] *Statement for the Record: Hearing on Worldwide Threat Assessment of the US Intelligence Community Before the S. Select Comm. on Intelligence*, 115th Cong. 1 (2017) (statement of Daniel R. Coats, Director of National Intelligence).

[2] *See* Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 233, 235 (2016); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, 5 J.L. & CYBER WARFARE 1, 3–4 (2015); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, U. ILL. J.L. TECH. & POL'Y 341, 345–47 (2015); Lawrence J. Trautman, *Following the Money: Lessons from the Panama Papers, Part 1: Tip of the Iceberg*, 121 PENN ST. L. REV. 807, 810 (2017).

[3] *See* THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, PRESIDENTIAL POLICY DIRECTIVE—CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [hereinafter PRESIDENTIAL POLICY ON INFRASTRUCTURE SECURITY].

[4] *See* Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR (Mar. 2, 2011, 12:00 AM), https://www.vanityfair.com/news/2011/03/stuxnet-201104.

By the year 2020, experts estimate 30 billion Internet of Things (IoT) devices will exist.[5] The IoT global market spend is estimated to "grow from $591.7 billion in 2014 to $1.3 trillion in 2019 with a compound annual growth rate of 17%."[6] And "[t]he installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019."[7] With this tremendous growth in both data and devices, a security nightmare is far more likely than not.

The proliferation of novel consumer devices and increased Internet-dependent business and government data systems introduces vulnerabilities of unprecedented magnitude.[8] Digital vulnerabilities touch upon a number of different areas of the law: privacy,[9] risk management,[10] corporate governance[11] (including the duties of

---

[5] *See* VERIZON, STATE OF THE MARKET: INTERNET OF THINGS 2016 3 (2016), https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf.

[6] *Id.*

[7] *Id.*

[8] *See* Trey Herr & Allan Friedman, *Redefining Cybersecurity*, 8 AM. FOREIGN POL'Y COUNCIL – DEF. TECH. PROGRAM BRIEF 1, 1–2 (2015); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1, 23–24 (2003).

[9] *See* Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, *in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 272, 283 (F. Xavier Olleros & Majlinda Zhegu eds., 2016); Corey Ciocchetti, *The Privacy Matrix*, 12 U. FLA. J. TECH. L. & POL'Y 245, 249 (2007); Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1064–65 (2009); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590 (2014); Robert Kirk Walker, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257, 269–70 (2012); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 2.0)* 3 (George Washington Law Sch. Pub. Law Research Paper No. 132, 2005).

[10] *See* Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 8–9 (2014); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance*, 6–7 (Legal Studies Research Paper Series No. 2017-23, 2017).

[11] *See* Lucian Bebchuk et al., *What Matters in Corporate Governance?*, 22 REV. FIN. STUD. 783, 788 (2009); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 315–17 (2011); John Armour et al., *Agency Problems, Legal Strategies, and Enforcement* 9, 11–12 (John M. Olin Ctr. for Law, Econ., & Bus., Working Paper No. 644, 2009).

care,[12] monitor,[13] and disclosure[14]), breach notification,[15] information and data security,[16] securities regulation,[17] law of war,[18] constitutional provisions,[19] and more.[20] This Article adds to our under-

---

[12] *See* Stephen M. Bainbridge et al., *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559, 574–75 (2008); Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1780–81 (2001); Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 1, 11 (2006).

[13] *See* Robert T. Miller, *The Board's Duty to Monitor Risk After* Citigroup, 12 U. PA. J. BUS. L. 1153, 1154–55 (2010).

[14] *See* Bernard S. Black, *The Core Fiduciary Duties of Outside Directors*, 3 ASIA BUS. L. REV. 1, 18–19 (2001); Henry T. C. Hu, *Too Complex to Depict? Innovation, "Pure Information," and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601, 1614–15 (2012); Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1344–45 (2006).

[15] *See* Dana J. Lesemann, *Once More unto the Breach: An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes*, 4 AKRON INTELL. PROP. J. 203, 206–08 (2010); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 918, 923–25 (2007); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1, 1–2 (2009); Fabio Bisogni, *Evaluating Data Breach Notification Laws. What Do the Numbers Tell Us?* 2 (Aug. 15, 2013) (unpublished manuscript), https://ssrn.com/abstract=2236144.

[16] *See* Ian Brown et al., *Information Security and Cybercrime*, *in* LAW AND THE INTERNET 671, 671 (Lilian Edwards & Charlotte Waelde eds., 3d ed. 2009); Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 111 (Anupam Chander et al. eds., 2008); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1708–11 (2010); Richard Warner & Robert H. Sloan, *Defending Our Data: The Need for Information We Do Not Have* 1–2 (Aug. 11, 2016) (unpublished manuscript), https://ssrn.com/abstract=2816010; Josephine Wolff, *Models for Cybersecurity Incident Information Sharing and Reporting Policies* 3 (Aug. 13, 2014) (unpublished manuscript), https://ssrn.com/abstract=2587398.

[17] *See* Zohar Goshen & Gideon Parchomovsky, *The Essential Role of Securities Regulation*, 55 DUKE L.J. 711, 732–37 (2006); Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 136–37 (2005); Robert B. Thompson & Hillary A. Sale, *Securities Fraud as Corporate Governance: Reflections upon Federalism*, 56 VAND. L. REV. 859, 869–70 (2003); Lawrence J. Trautman & George P. Michaely, Jr., *The SEC & the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262, 262–63 (2014).

standing of the development of cyber vulnerabilities resulting directly from: (1) the Stuxnet code and its progeny, and (2) widespread malware exposure associated with the IoT.

This Article proceeds in eight parts. First, we provide an overview of the industrial cyber vulnerability problem. Second, we explain a chief problem: digital vulnerabilities in industrial systems. Third, we relate a diverse variety of sources of cybersecurity-related legal obligations—including corporate duties, data privacy statutes, and consumer-protection litigation, among others. Fourth is a discussion of the history of the Stuxnet malware—which targeted a ubiquitous, industrial-control device called programmable logic controllers (PLCs)—and implications for the future. Fifth, we examine the recent development of the Internet of things—its current status, known vulnerabilities, and likely future. Sixth is a discussion of continued exposure of intelligence agency's cyber toolsets. Seventh, we suggest topics for future research. We then conclude with some final thoughts.

---

[18] *See* DANIEL SUI ET AL., WILSON CTR. SCI. & TECH. INNOVATION PROGRAM, THE DEEP WEB AND THE DARKNET: A LOOK INSIDE THE INTERNET'S MASSIVE BLACK BOX 11–12 (2015); Christopher S. Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 175, 191–93 (Jens David Ohlin et al. eds., 2015); Steven M. Bellovin et al., *Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications*, 3 J. CYBERSECURITY 59, 60 (2017); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 209–12 (2002); Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEX. INT'L L.J. 189, 224–25 (2015); Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 3, 25–27 (2016); Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. (forthcoming 2017) (manuscript at 2–3), https://ssrn.com/abstract=2932110.

[19] *See* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALBANY L.J. SCI. & TECH. (forthcoming 2018) (manuscript at 15).

[20] *See* TREY HERR ET AL., BELFER CTR. FOR SCI. & INT'L AFFAIRS, THE CYBER SECURITY PROJECT, TAKING STOCK: ESTIMATING VULNERABILITY REDISCOVERY (2017) (discussing vulnerabilities in software).

II. THE INDUSTRIAL CYBER VULNERABILITY PROBLEM

What we're seeing now is a lot of intrusions. We're seeing a lot of infiltrations . . . and then the next step is, again, the disruptive, disabling, destructive types of attacks. And so . . . electric grids, water treatment facilities . . . mass transportation systems . . . railways and trains, whatever — if those intruders get into those systems and then can determine how they can in fact interfere in the command and control systems of these systems, they . . . could . . . put trains onto the same tracks. They can . . . bring down electric grids . . . .

John Brennan
Former Assistant to the President for Homeland Security and Counter-terrorism; Former Director, Central Intelligence Agency[21]

Critical infrastructure is defined in the USA PATRIOT Act[22] as "systems and assets, . . . physical or virtual, so vital to the United States 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

---

[21] *See* Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230, 254–55 (2016) (quoting Ritika Singh, *Transcript of John Brennan's Speech on Yemen and Drones*, LAWFARE (Aug. 9, 2012, 2:38 PM), http://www.lawfareblog.com/2012/08/transcript-of-john-brennans-speech-at-the-council-on-foreign-relations).

[22] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 2001 U.S.C.C.A.N. (115 Stat.) 272 (2001).

matters."[23] It was Presidential Decision Directive 63 (or PDD-63)[24] that identified the requirement to protect the following critical infrastructures: "information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production; and storage."[25] The following four activities controlled by the federal government were specifically identified by PDD-63: "(1) internal security and federal law enforcement; (2) foreign intelligence; (3) foreign affairs; and (4) national defense."[26]

The Obama Administration issued PPD-21, or *Critical Infrastructure Security and Resilience*, in February 2013.[27] PPD-21 directed the federal government to "work with critical infrastructure owners and operators . . . to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, [or] public health and safety."[28]

---

[23] *Id.* § 1016(e); *see* RITA TEHAN, CONG. RESEARCH SERV., R44410, CYBERSECURITY: CRITICAL INFRASTRUCTURE AUTHORITATIVE REPORTS AND RESOURCES 1 n.1 (2017) ("This included causing catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction; impairing federal agencies' abilities to perform essential missions or ensure the public's health and safety; undermining state and local government capacities to maintain order and deliver minimum essential public services; damaging the private sector's capability to ensure the orderly functioning of the economy; having a negative effect on the economy through cascading disruption of other infrastructures; or undermining the public's morale and confidence in our national economic and political institution. HSPD-7 has since been superseded by PDD-21."); *see also Homeland Security Presidential Directive 7; Critical Infrastructure Identification, Prioritization, and Protection*, U.S. DEP'T. OF HOMELAND SEC. (Dec. 17, 2003), https://www.dhs.gov/homeland-security-presidential-directive-7 (describing the asset loss impact level necessary to deem the asset as "critical").

[24] Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804 (Aug. 5, 1998).

[25] *See* TEHAN, *supra* note 23, at 1.

[26] *Id.*

[27] *Id.* (citing PRESIDENTIAL POLICY ON INFRASTRUCTURE SECURITY, *supra* note 3).

[28] PRESIDENTIAL POLICY ON INFRASTRUCTURE SECURITY, *supra* note 3.

On May 11, 2017, President Trump signed an executive order intended to improve the federal government's cybersecurity and protect critical infrastructure from digital attacks.[29] The most "notable changes" include requiring "heads of federal agencies [to] use a framework developed by the National Institute of Standards and Technology to assess and manage cyber risk, and prepare a report within 90 days documenting how they will implement it."[30]

Unlike most other nations, in the United States the private sector owns and operates an estimated 90% of the nation's critical infrastructure.[31] Other significant elements of U.S. critical national infrastructure include those maintained by federal agencies, such as air traffic control systems, and materials handling operations, such as mail sorting by the U.S. Postal Service.[32]

A. *Industrial Control Systems*

Industrial control systems (ICS) are ripe targets for digital attack. ICS include: "supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)."[33] These control systems are vital to the functionality of the U.S. critical infrastructures, which "are often highly interconnected and mutually dependent systems."[34]

ICS are used in a wide swath of industries, including: "electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods)."[35]

---

[29] Dustin Volz, *Trump Signs Order Aimed at Upgrading Government Cyber Defenses*, REUTERS (May 11, 2017, 1:35 PM), http://www.reuters.com/article/us-usa-trump-cyber-idUSKBN1872L9.

[30] *Id.*

[31] *See* U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY 1 (2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (rev. 2) [hereinafter GUIDE TO ICS SECURITY].

[32] *See id.*; *see Critical Infrastructure Sectors*, U.S. DEPT. OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-sectors (last updated July 11, 2017).

[33] GUIDE TO ICS SECURITY, *supra* note 31, at 1.

[34] *Id.*

[35] *Id.*

Generally, SCADA systems are "used to control dispersed assets using centralized data acquisition and supervisory control."[36] DCS are "used to control production systems within a local area such as a factory using supervisory and regulatory control."[37] Finally, PLCs are "used for discrete control for specific applications and generally provide regulatory control."[38]

Cyber threats initially did not pose a risk to ICS, because "ICS were [typically] isolated systems running proprietary control protocols using specialized hardware and software" and their "components were in physically secured areas and the components were not connected to IT networks or systems."[39] But as the Internet Protocol devices proliferate and decrease in price, they have begun to replace proprietary ICS components—significantly increasing vulnerabilities to digital attacks.[40]

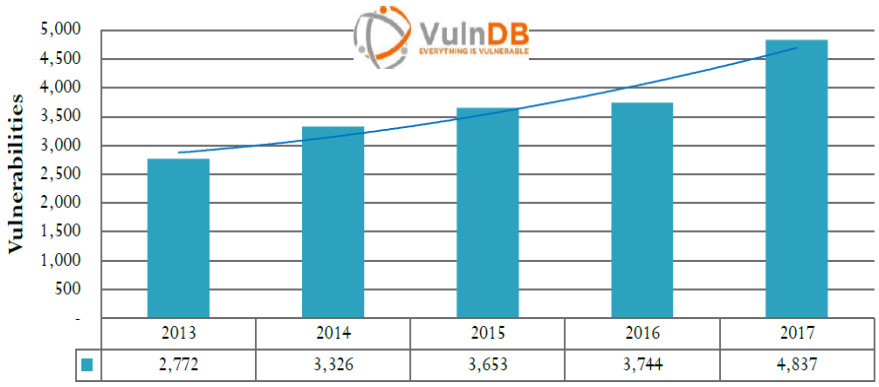
B. *Vulnerabilities Escalate*

By the first quarter of 2017, an all-time high number of disclosed vulnerabilities had been reached.[41] Risk Based Security observes: "While no significant increase occurred from 2014 to 2016, the number of disclosed vulnerabilities jumped (29.2%) in Q1 2017."[42] Risk Based Security also notes that if this trend continues, then 2017 is on "the path to become a record-breaking year in the number of vulnerabilities disclosed!"[43] Exhibit 1 below provides a comparison of first quarter vulnerabilities over a five-year period.

---

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *See id.*
[41] *See* RISK BASED SEC., VULNERABILITY QUICKVIEW: FIRST QUARTER 2017 VULNERABILITY TRENDS 3 (2017).
[42] *Id.*
[43] *Id.*

Exhibit 1
A Comparison of First Quarter 2017
Vulnerabilities to the Past Four Years[44]



Source: Risk Based Security, Inc.

Statistics for the first quarter of 2017 reveal that the largest target of attack traffic is the United States, "with Brazil in second place for the second quarter in a row," and the United Kingdom in third.[45] Furthermore, "[a]ttacks targeting the U.S. were down 9%, while Brazil saw a nearly 46% increase in web application attacks . . . and the U.K. a 30% gain."[46] Exhibit 2 depicts the Top 10 Target Countries for Web Application Attacks, Q1 2017.

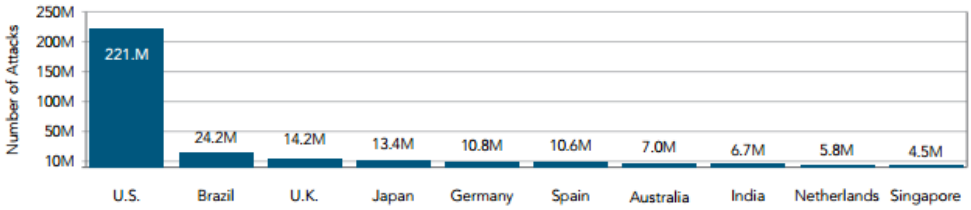
---

[44] *Id.*

[45] AKAMAI TECHS., STATE OF THE INTERNET / SECURITY Q1 2017 REPORT 16 (Martin McKeay & Amanda Fakhreddine eds., 2016), https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf.

[46] *Id.*

Exhibit 2
Top 10 Target Countries for Web Application Attacks,
Q1 2017[47]



Source: Akamai

III. THE CYBERSECURITY LEGAL FRAMEWORK

Cybersecurity law and compliance with legal obligations is particularly difficult because there is no single source of authority—such as a comprehensive federal statute or regulation—that exhaustively lists legal obligations and duties. Instead, cybersecurity legal obligations are "set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as in common law duties, contractual commitments, and other expressed and implied obligations to provide 'reasonable' or 'appropriate' security."[48] In this section, we review a trio of corporate data security legal obligations and then turn to address several other cybersecurity-related legal subjects.

A. *Corporate Duties of Loyalty and Care*

Because so much of U.S. critical infrastructure and cyber risk is in the hands of private corporations, effective governance of these entities is imperative. At the foundation of our system of corporate governance, corporate directors have two primary duties: (1) the

---

[47] *Id.*

[48] THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 29 (2008).

duty of loyalty (to place the corporate interest ahead of self-interest);[49] and (2) the duty of care.[50] Subsets of the duty of care include

[49] *See* Larry Catá Backer, *Director Independence and the Duty of Loyalty: Race, Gender, Class and the Disney-Ovitz Litigation*, 79 ST. JOHN'S L. REV. 1011, 1026–27 (2005); Bainbridge et al., *supra* note 12, at 564; Blair & Stout, *supra* note 12, at 1758–59; J. Robert Brown, Jr., *Disloyalty Without Limits: "Independent" Directors and the Elimination of the Duty of Loyalty*, 95 KY. L.J. 53, 58–60 (2006); Christopher M. Bruner, *Good Faith, State of Mind, and the Outer Boundaries of Director Liability in Corporate Law*, 41 WAKE FOREST L. REV. 1131, 1132 (2006); Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925, 936–40 (2006); Eisenberg, *supra* note 12, at 4–6; Goshen & Parchomovsky, *supra* note 17, at 717–19; Stephanie Greene & Christine Neylon O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281, 285–87 (2013); Darian M. Ibrahim, *Individual or Collective Liability for Corporate Directors?*, 93 IOWA L. REV. 929, 955–57 (2008); Gabriel Rauterberg & Eric Talley, *Contracting Out of the Fiduciary Duty of Loyalty: An Empirical Analysis of Corporate Opportunity Waivers*, 117 COLUM. L. REV. 1075, 1084–86 (2017); Kenneth M. Rosen, *Fiduciaries*, 58 ALA. L. REV. 1041, 1046–48 (2007); Hillary A. Sale, *Delaware's Good Faith*, 89 CORNELL L. REV. 456, 463 (2004); Leo E. Strine, Jr., et al., *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law*, 98 GEO. L.J. 629, 635–36 (2010); Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1213, 1239–40 (2010); Armour et al., *supra* note 11, at 2.

[50] *See* William T. Allen, *Modern Corporate Governance and the Erosion of the Business Judgment Rule in Delaware Corporate Law*, 4 COMP. RES. L. & POL. ECON. 1, 10–11 (2008); Douglas M. Branson, *The Rule That Isn't a Rule - the Business Judgment Rule*, 36 VAL. U. L. REV. 631, 634–35 (2002); Gregory Scott Crespi, *Standards of Conduct and Standards of Review in Corporate Law: The Need for Closer Alignment*, 82 NEB. L. REV. 671, 671–72 (2004); Lisa M. Fairfax, *Spare the Rod, Spoil the Director? Revitalizing Directors' Fiduciary Duty Through Legal Liability*, 42 HOUS. L. REV. 393, 409–11 (2005); Lyman P. Q. Johnson & David Millon, *Recalling Why Corporate Officers Are Fiduciaries*, 46 WM. & MARY L. REV. 1597, 1630 (2005); Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting* Corporate Law*'s "Duty of Care as Responsibility for Systems"*, 31 J. CORP. L. 949, 953 (2006); Stephen J. Lubben & Alana J. Darnell, *Delaware's Duty of Care*, 31 DEL. J. CORP. L. 589, 594–95 (2006); Holger Spamann, *Monetary Liability for Breach of the Duty of Care?*, 8 J. LEGAL ANALYSIS 337, 337–38 (2016); Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, 1 AM. U. BUS. L. REV. 337, 340 (2012).

the duties to monitor and to be informed. Recently, we have contributed to the corporate governance literature by expanding on the concept of a corporate cybersecurity standard of care.[51]

Elsewhere, we observe that "[t]he duty of care is a concept adapted from tort law, and it requires an actor to behave reasonably."[52] Director liability for a breach of the duty of care may arise in two distinct contexts.[53] First, liability may "follow from a board decision that results in a loss because that decision was ill advised or 'negligent.'"[54] Second, liability may "arise from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."[55]

B. *Corporate Duty to Monitor*

At its core, a breach of the duty to monitor arises when "a loss eventuates not from a decision but, from unconsidered inaction."[56] Observing that "[m]ost of the decisions that a corporation, acting through its human agents, makes are . . . not the subject of director attention," the court in *Caremark* nonetheless recognized that "ordinary business decisions that are made by officers and employees deeper in the interior of the organization can . . . vitally affect the welfare of the corporation and its ability to achieve its various strategic and financial goals."[57]

To satisfy their obligation to be reasonably informed, corporate boards at a minimum must "assur[e] themselves that information

---

[51] *See* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1280 (2017) [hereinafter Trautman & Ormerod, *Yahoo Data Breach*].

[52] *Id.* at 1245 (citing Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139, 1159–60 (2013)). *See also* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 303, 315–16 (2015).

[53] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

[54] *Id.*

[55] *Id.* (citing E. Norman Veasey & Julie M.S. Seitz, *The Business Judgment Rule in the Revised Model Act, the* Trans Union *Case, and the ALI Project—A Strange Porridge*, 63 TEX. L. REV. 1483, 1486 (1985)).

[56] *Id.* at 968.

[57] *Id.*

and reporting systems exist in the organization that are reasonably designed to provide . . . timely, accurate information sufficient to allow management and the board . . . to reach informed judgments concerning . . . the corporation's compliance with law."[58] This is not to say that there is a universal, one-size-fits-all solution to the duty to monitor—"the level of detail that is appropriate for such an information system is a question of business judgment."[59] Nor does the mere existence of an adequate monitoring system eliminate the risk "that the corporation will violate laws or regulations, or that senior officers or directors may nevertheless sometimes be misled or otherwise fail reasonably to detect acts material to the corporation's compliance with the law."[60]

Accordingly, the duty to monitor requires "the board [to] exercise a good faith judgment that the corporation's information and reporting system is in *concept and design* adequate to assure the board that appropriate information will come to its attention in a timely manner."[61] Therefore, to avoid liability and to conform to relevant legal norms, directors should make a good faith attempt to ensure the company has a "corporate information gathering and reporting system" that the board finds satisfactory.[62] In summary, the corporate law duty of care centers on whether corporate directors and officers employed a "good faith effort" to remain reasonably informed sufficient to exercise good judgment.[63]

---

58 *Id.* at 970.

59 *Id.*

60 *Id.*

61 *Id.* (emphasis added).

62 *Id.* at 969.

63 *Id.* at 970; *see also* William T. Allen et al., *Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique of* Van Gorkom *and Its Progeny as a Standard of Review Problem*, 96 NW. U. L. REV. 449, 457 n.31 (2002) (stating that "directors will not be held liable" for a breach of the duty to monitor without a finding of bad faith); Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does It Matter?*, 48 WAKE FOREST L. REV. 1027, 1046–47 (2013) (asserting that liability under the *Caremark* standard requires bad intentions toward the company, such as a "total board failure to engage in oversight"); Lynn A. Stout, *In Praise of Procedure: An Economic and Behavioral Defense of* Smith v. Van Gorkom *and the Business Judgment Rule*, 96 NW. U. L. REV. 675, 680 (2002) (noting that in some states, directors are presumed to meet the duty of care if the decision was "informed,"

C. *Corporate Duty to Disclose*

At least two distinct authorities require that a publicly traded corporation has a duty to disclose the existence of a data breach: (1) Delaware state corporate common law, and (2) the SEC's 2011 corporate finance disclosure guidance, which identifies material data security risks that companies must disclose under securities law disclosure requirements and accounting standards.[64] Therefore, companies that know about a data breach but fail to disclose it to shareholders, regulators, and consumers, risk liability under potentially corporate, breach notification, and securities laws.

Well established in Delaware common law is the concept that directors and officers of a corporation have a fiduciary duty to shareholders and the corporation of disclosure—sometimes referred to as a duty of complete candor.[65] Over two decades ago, Professor Lawrence A. Hamermesh noted that Delaware courts have recognized "that a fiduciary duty to disclose all material information arises when directors approve any public statement, such as a press release, regardless of whether any specific stockholder action is sought."[66] Director negligence is irrelevant in assessing the duty to disclose.[67] The duty serves two purposes: (1) "to afford stockholders a remedy," regardless of whether they relied upon a misstatement or omission, and (2) "to afford a 'virtual *per se* rule' of damages," awarding stockholders a monetary award "without having to establish actual loss."[68] In sum, the duty to disclose in Delaware requires that directors provide shareholders with "all material information" about the

---

and "unless the directors had been . . . *grossly* negligent in failing to inform themselves, before acting," courts deem the decision to be informed).

[64] *See* U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2: CYBERSECURITY (2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [hereinafter SEC CF DISCLOSURE GUIDANCE]; Lawrence A. Hamermesh, *Calling Off the* Lynch *Mob: The Corporate Director's Fiduciary Disclosure Duty*, 49 VAND. L. REV. 1087, 1089–90 (1996).

[65] Hamermesh, *supra* note 64, at 1097 & nn.34–35.

[66] *Id.* at 1091.

[67] *See id.*

[68] *Id.*

corporation whenever they communicate with the shareholder or market, even if the shareholder did not request it.[69]

Guidance provided during 2011 by the SEC's division of corporation finance notes that "federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision."[70] Although the Guidance acknowledges that "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," the SEC nonetheless required the disclosure of "material information regarding cybersecurity risks and cyber incidents" to prevent misleading the public.[71] The Guidance provides several examples of situations in which corporate disclosure is mandatory. First, the Guidance provides that it "expect[s] registrants to evaluate their cybersecurity risks and take into account all available relevant information, including *prior cyber incidents and the severity and frequency of those incidents*."[72] Second, the Guidance advises that:

> [r]egistrants should address cybersecurity risks and cyber incidents . . . if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition.[73]

The Industrial Internet provides management with an enhanced capability to mitigate enterprise risk. As Greengard observes, given "the right software and dashboard in place, it's possible to view data across an entire physical infrastructure. In other words, an agency or organization could clearly determine—based on structural data

---

[69] Shannon German, *What They Don't Know Can Hurt Them: Corporate Officers' Duty of Candor to Directors*, 34 DEL. J. CORP. L. 221, 233 (2009); *see also* Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L.J. 205, 228 (2013) [hereinafter Trautman, *Who Qualifies as an Audit Committee Financial Expert?*].

[70] SEC CF DISCLOSURE GUIDANCE, *supra* note 64.

[71] *Id.*

[72] *Id.* (emphasis added).

[73] *Id.*

rather than opinions and politics—the real world risks and costs of fixing or ignoring a problem."[74]

D. *Challenge to Corporate Governance*

Recent years have shown, as well as in these pages to follow, that "[f]ew enterprise operational areas present as much inherent risk or prove as difficult to govern as Information Technology" (IT).[75] Not many corporate directors have an engineering, data, or information technologies background that prepares the director to bring an expert viewpoint based upon knowledge and experience about cybersecurity issues to boardroom risk discussions. In recognition of this critically important board responsibility for risk management, "new SEC rules went into effect on February 28, 2010 amending Item 407 of Regulation S-K to require disclosure about the board's role in a company's risk oversight process and its leadership structure."[76] The SEC states that the new disclosure rules require "companies . . . to describe how the board administers its risk

---

[74] *See* SAMUEL GREENGARD, THE INTERNET OF THINGS 66 (2015).

[75] *See* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75, 112 (2012) [hereinafter Trautman, *The Matrix*]; Lawrence J. Trautman, *Who Sits on Texas Corporate Boards? Texas Corporate Directors: Who They Are and What They Do*, 16 HOUS. BUS. & TAX L.J. 44, 94–95 (2016); Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 261, 263–64 (2016) [hereinafter Trautman, *Lessons from Paypal*]; Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275, 324 (2017); Lawrence J. Trautman, Anthony (Tony) J. Luppino & Malika Simmons, *Some Key Things U.S. Entrepreneurs Need to Know About the Law and Lawyers*, 46 TEX. J. BUS. L. 155, 172 (2016); Trautman, *Who Qualifies as an Audit Committee Financial Expert?*, *supra* note 69, at 232.

[76] *See* Trautman, *The Matrix*, *supra* note 75, at 113 & n.84 (quoting Trautman & Altenbaumer-Price, *supra* note 11, at 317 & n.15) ("The text of the new rule reads: (h) Board leadership structure and role in risk oversight. Briefly describe the leadership structure of the registrant's board, such as whether the same person serves as both principal executive officer and chairman of the board, or whether two individuals serve in those positions, and, in the case of a registrant that is an investment company, whether the chairman of the board is an 'interested person' of the registrant as defined in section 2(a)(19) of the Investment Company Act (15 U.S.C. 80a-2(a)(19)). If one person serves as both principal executive officer and chairman of the board, or if the chairman of the board of a registrant that is an investment company is an 'interested person' of the registrant, disclose whether the registrant has a lead independent director and what specific role the

oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."[77] Disclosures should address, for example, "whether the individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee or how the board or committee otherwise receives information from such individuals."[78] Such disclosures should also include an explanation of the board's leadership structure and the "reasons why" the company believes that this board leadership structure is the most "appropriate structure for the company."[79] In companies in which the CEO and Chairman are the same individual, rule "amendments will require disclosure of whether and why the company has a lead independent director, as well as the specific role the lead independent director plays in the leadership of the company."[80]

E. *Other Relevant Legal Authorities*

As discussed briefly above, data privacy legal obligations are the byproduct of an exceptionally complex web of statutes, rules, and regulations of a dizzying array of sources. A non-comprehensive list of these sources follows below.

1. STATUTES AND REGULATIONS

These include: "privacy laws, data security laws, electronic transaction laws, corporate governance laws, unfair and deceptive business practice and consumer protection laws, and breach notification laws."[81]

---

lead independent director plays in the leadership of the board. This disclosure should indicate why the registrant has determined that its leadership structure is appropriate given the specific characteristics or circumstances of the registrant. In addition, disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure.").

77 U.S. SEC. & EXCH. COMM'N, RELEASE NOS. 33-9089, 34-61175, IC-29092, PROXY DISCLOSURE ENHANCEMENTS (Feb. 28, 2010), http://sec.gov/rules/final/2009/33-9089.pdf.

78 *Id.*

79 *Id.*

80 *Id.*; *see also* Trautman & Michaely, *supra* note 17, at 278.

81 Trautman & Ormerod, *Yahoo Data Breach*, *supra* note 51, at 1235.

On the federal level, privacy statutes include: Financial Services Modernization Act of 1999, which concerns the financial sector;[82] the Health Insurance Portability and Accountability Act of 1996, which concerns healthcare information;[83] the Privacy Act of 1974, which establishes governmental record-keeping requirements;[84] and the Children's Online Privacy Protection Act, which applies to all businesses that collect personal information on the Internet from children.[85]

Some federal regulations also require organizations to protect specific types of data; these include IRS revenue procedures requiring security measures to protect electronic tax records[86] and SEC regulations requiring the protection of corporate financial data.[87] Federal banking regulations also impose an obligation on financial institutions to disclose security breaches.[88]

The U.S. Federal Trade Commission has been particularly active enforcing data security obligations. Section 5 of the Federal Trade Commission Act (FTC Act),[89] associated Federal Trade Commission enforcement actions, and equivalent state statutes are the chief

---

[82] *See* Financial Services Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); *see generally* Timothy J. Yeager et al., *The Financial Services Modernization Act: Evolution or Revolution?*, 59 J. ECON. & BUS. 313 (2007).

[83] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 and 42 U.S.C.).

[84] Privacy Act of 1974, 5 U.S.C. § 552a (b) (2012).

[85] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–02 (2012).

[86] *See* Rev. Proc. 97-22, 1997-1 C.B. 652; Rev. Proc. 98-25, 1998-1 C.B. 689.

[87] *See* 17 C.F.R. § 248.30 (2004); 17 C.F.R. § 257.1(e)(3) (2011).

[88] *See* Supplement A to Appendix B to Part 30, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. pt. 30 (2017); *see* Supplement A to Appendix D-2 to Part 208-Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice, 12 C.F.R. pt. 208 (2017); *see* Supplement A to Appendix B to Part 364-Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. pt. 364 (2017) (reviewing commentator feedback on agency proposed guidance for how institutions should respond and notify consumers following unauthorized access to consumer information).

[89] *See* 15 U.S.C. § 45 (2012).

sources for the imposition of consumer protection data security obligations. From 2005 through the present, the FTC has aggressively pursued a broad interpretation of the law in its cybersecurity-related enforcement actions by contending that a company's failure to provide appropriate data security for consumers' personal information was, alone, an unfair (not deceptive) trade practice.[90] That is, a company could be liable without ever having misrepresented the extent of its data security practices to consumers.[91] Subsequently, in August 2015, the Third Circuit ratified the FTC's broader theory of liability.[92]

On the state level, several states have enacted data security statutes that impose a general obligation on all companies to ensure the security of personal information.[93] Moreover, forty-seven states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have also enacted cybersecurity breach notification laws, which impose an obligation to disclose security breaches to those affected.[94]

---

[90] *See Discussion Draft of H.R.__, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach*, 112th Cong. 44 (2011) (statement of Edith Ramirez, Comm'r, FTC) ("[T]he Commission enforces the FTC Act's proscription against unfair . . . acts . . . in cases where a business['s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury."); *see The Threat of Data Theft to American Consumers: Hearing Before the S. Comm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 15 (2011) (statement of David C. Vladeck, Dir., Bureau of Consumer Prot., FTC) (same).

[91] *See* Children's Online Privacy Protection Act, *supra* note 85.

[92] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–47, 249, 259 (3d Cir. 2015) (holding that Wyndham's failure to secure consumer information, which resulted in actual harm to consumers, fell within the plain meaning of "unfair").

[93] *See* CAL. CIV. CODE § 1798.81.5(b) (West 2016); *see also* SMEDINGHOFF, *supra* note 48, at 5.

[94] *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATORS, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Feb. 6, 2018).

2. COMMON LAW

While commentators have long contended there is, at the very least, a "common law duty to provide adequate security for corporate data,"[95] courts have only more recently explicitly agreed. In 2005, for instance, a state appellate court in *Bell v. Michigan Council 25*[96] held that the "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[97]

And, more recently, a federal district court held:

> Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.[98]

---

[95] SMEDINGHOFF, *supra* note 48, at 31 (citing Kimberly Kiefer & Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, 1 BNA PRIVACY & SECURITY L. REP. 788 (2002); Alan Charles Raul et al., *Liability for Computer Glitches and Online Security Lapses*, 6 BNA ELEC. COMMERCE L. REP. 849 (2001); Erin Kenneally, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, 16 COMPUTER SECURITY J. 1 (2000)).

[96] No. 246684, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005) (per curiam).

[97] *Id.* at *5.

[98] *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (citations omitted); *see generally* Lawrence J. Trautman, The SONY Data Hack: Implications for World Order (unpublished manuscript) (on file with author).

3. CONTRACTUAL OBLIGATIONS

When third parties have possession of, control over, or access to corporate data, companies that entrust third parties to manage their data are increasingly trying to satisfy their duty to protect the security of their data by contract.[99]

4. SELF-IMPOSED OBLIGATIONS

Finally, companies have also imposed requirements on themselves. In addition to the FTC's unfair theory of cybersecurity liability, the agency also aggressively enforces representations that organizations make about their own security practices under a deceptive trade practice theory.[100]

5. CONSTITUTIONAL PROVISIONS

A comprehensive review of the multitude of U.S. Constitutional issues implicated by the fast-developing digital threats reviewed below is beyond the scope of this paper and will likely be the topic of a future body of scholarly work from us. Given the space limitations provided to a single law journal article, we can do little more here than provide a modest list of a few of the major issues implicated. These topics include: First Amendment;[101] Third Amendment;[102]

---

[99] SMEDINGHOFF, *supra* note 48, at 33.

[100] *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (holding that in light of Wyndham's publication of a privacy policy, in which it promised to protect consumers' personal information, the failure to implement corresponding security measures amounted to an unfair practice under the FTC Act).

[101] *See* Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 3–4 (2007).

[102] *See* Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203, 1206–07, 1227 (2013).

Fourth Amendment;[103] Broadcast regulation;[104] copyright law issues;[105] legality of war;[106] and privacy.[107]

F. *The Cybersecurity Standard of Care*

Evolving concepts of cyber specific law remain challenged by the rapid pace of developing technologies.[108] Elsewhere, we have presented a detailed discussion outlining the concept of Corporate Directors' and Officers' Cybersecurity Standard of Care, in part as a response to the recent Yahoo Data Breaches.[109]

As noted above and throughout this section, there is no one, single, comprehensive cybersecurity statute or regulation. This patchwork of authorities has given rise to a one-size-fits-all process-ori-

---

[103] *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 825–26 (2016); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 626–27 (2011); *see also* Ormerod & Trautman, *supra* note 19 (manuscript at 15).

[104] *See* Thomas Fetzer & Christopher S. Yoo, *New Technologies and Constitutional Law*, *in* ROUTLEDGE HANDBOOK OF CONSTITUTIONAL LAW 485, 486 (Mark Tushnet et al. eds., 2013).

[105] *See* Lidiya Mishchenko, *The Internet of Things: Where Privacy and Copyright Collide*, 33 SANTA CLARA HIGH TECH. L.J. 90, 100 (2016).

[106] *See* Gary D. Brown & Andrew O. Metcalf, *Easier Said than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 118–20 (2014); Christopher S. Yoo, *Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 175, 191–93 (Jens David Ohlin et al. eds., 2015); Carol M. Hayes & Jay P. Kesan, *Law of Cyber Warfare* 2 (Ill. Pub. Law & Legal Theory, Research Paper Series No. 14-26, 2014), https://ssrn.com/abstract=2396078.

[107] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1, 2 (2015).

[108] *See* Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232, 232–33 (2016); Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041, 1050 (2017); Trautman, *Lessons from Paypal*, *supra* note 75, 282–83; Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 1, 2 (2014); Lawrence J. Trautman, How Google Perceives Customer Privacy, Cyber, E-commerce, Political and Regulatory Compliance Risks 5–6 (2018) (unpublished manuscript).

[109] *See* Trautman & Ormerod, *Yahoo Data Breach*, *supra* note 51, at 1234–35.

ented approach to organizational data security: the Written Information Security Program (WISP).[110] This "emerging digital security standard is particularized and case specific," and that, "[u]nlike prior specific requirements, such as passwords or firewalls, the new corporate security obligation is fact-specific, requiring companies to go through a 'process' and determine what security measures are most appropriate for the company's security needs."[111] Under the WISP protocol, organizations create their own specific security measures and are required to "conduct ongoing reviews of their security mechanisms."[112] "This repetitive review process includes detecting and evaluating risks, implementing specific security responses to those risks, verifying the effective implementation of those security responses, and updating the measures as needed in reaction to developing security concerns."[113]

The seven steps of a comprehensive WISP protocol are:

> *Assign Responsibility*: A corporation should expressly designate one or more employees to be responsible for maintaining the data security program.
>
> *Identify Information Assets*: A corporation should identify its information assets that require protection, which include both the data itself (i.e., records containing personal information) and the computing systems that store the personal information (e.g., servers, laptops, and portable devices).
>
> *Conduct Risk Assessment*: A corporation should perform a risk assessment to identify both internal and external risks to its data security, and it should evaluate the effectiveness of the company's current practices for safeguarding and minimizing the risks identified.

---

110 Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 11 (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323.

111 Trautman & Ormerod, *Yahoo Data Breach*, *supra* note 51, at 1241 (citing Smedinghoff, *supra* note 110, at 9–10).

112 *Id.*

113 *Id*. at 1241–42.

> *Select and Implement Responsive Security Controls*: A corporation should implement physical, administrative, and technical security controls it considers appropriate to minimize the risks it identified in its risk assessment.
>
> *Monitor Effectiveness*: A corporation should *regularly* monitor, test, and reassess the security controls it has chosen to implement in order to ensure its security program is operating in a manner reasonably calculated to protect personal information. Relatedly, a corporation should regularly upgrade its security controls as necessary to limit emerging risks.
>
> *Regularly Review the Security Program*: A corporation should review and adjust its data security program no less than once per year. A corporation should also perform security program reviews whenever there is a material change in business practices that could affect personal information or after any incident involving a breach of its data security.
>
> *Address Third Party Issues*: A corporation should take all reasonable steps to verify that every third-party service provider that has access to the company's data assets and personal information has the capacity to protect that information.[114]

More and more authorities are endorsing the process-oriented approach of WISP for complex organizations facing myriad and diverse digital security difficulties. Of particular note is the recent adoption of the WISP protocol by a Federal Circuit Court of Appeals, an approached favored by the U.S. Federal Trade Commission.[115]

---

[114] *Id.* at 1242.

[115] *See id.* at 1243–45.

IV. STUXNET

Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. These threats are amplified by our ongoing delegation of decisionmaking, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events when they do occur.

Daniel R. Coats
Director of National Intelligence
May 11, 2017[116]

Digital threats to objects—and people—in the physical world increased by leaps and bounds in July 2010, when the world's foremost digital security experts discovered a computer virus radically different and far more sophisticated than any seen previously.[117] The mysteries of the virus's author and purpose unraveled throughout the end of 2010, and by early 2011 a single hypothesis had garnered widespread acceptance, which was confirmed in June 2012:[118] this piece of malware, dubbed "Stuxnet" (or code name Olympic Games)[119] was a covert joint operation between the United States

---

[116] *Statement for the Record: Hearing on Worldwide Threat Assessment of the US Intelligence Community Before the S. Select Comm. on Intelligence*, 115th Cong. 1 (2017) (statement of Daniel R. Coats, Director of National Intelligence).

[117] *See* Gross, *supra* note 4.

[118] *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[119] *See* ZERO DAYS (Magnolia Pictures 2016) (a documentary film by Alex Gibney depicting self-replicating computer malware used to destroy key parts of an Iranian nuclear facility and disclosing use of code name Olympic Games); *see also* Michael J. Glennon, *The Road Ahead: Gaps, Leaks, and Drips*, 89 INT'L L. STUD. U.S. NAVAL WAR C. 362, 363 (2013).

and Israel to sabotage Iranian centrifuges—industrial machines integral to the purification of radioactive uranium.[120] By modulating the speed that Iranian centrifuges spun, Stuxnet covertly devastated the machines from within—representing the first time the world "had seen digital code in the wild being used to physically destroy something in the real world."[121]

The ramifications of the Stuxnet virus are profound. Some have called Stuxnet "the first unattributable act of war."[122] Stuxnet represents a paradigm shift in how warfare could increasingly be waged in the 21st century.[123] Unlike traditional military clashes, these conflicts will take place in secret, over the Internet.[124] For the people whose lives depend on the targets of the cyber weapons, "the results could be as catastrophic as a bombing raid, but would be even more disorienting."[125]

Yet aside from these military implications, Stuxnet represents an entirely new type of weapon—a digital warhead capable of devastating tangible structures, systems, and the people that depend on them, far from a theater of battle.[126] Because Stuxnet exploited a tiny computer that is ubiquitous in modern industrial machinery, a virus similar to Stuxnet could have immensely harmful effects on industrialized nations' critical infrastructure.[127] The tiny computers Stuxnet commandeered were PLCs.[128] PLCs perform tasks as varied as opening and shutting valves in water pipes, timing the change of traffic lights, and dolloping out the appropriate amount of cream into

---

120 DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER x (2012); Derek E. Bambauer, *Schrödinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791, 794 (2015); William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

121 Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

122 Gross, *supra* note 4.

123 *Id.*

124 *Id.*

125 *Id.*

126 *See* Zetter, *supra* note 121.

127 Gross, *supra* note 4.

128 *Id.*

individual Oreo cookies.[129] Stuxnet's hijacking of the PLCs in Iranian centrifuges is a dire warning: the very basis of modern industrial life is an exploitable target for a cyber attack.

Stuxnet and its progeny have revealed the susceptibility of critical civilian infrastructure to digital attack. Details of the Stuxnet virus illuminate why the virus represents a dramatic shift in cyberwarfare. Understanding the novel threat that Stuxnet presents, critical infrastructure has nonetheless failed to address and fix the vulnerabilities that Stuxnet exploited. Further, the existing cyber-security legal framework in the United States may prove inadequate to address the challenges that Stuxnet presents.

A. *The Stuxnet Virus*

On June 17, 2010, Sergey Ulasen, the head of an anti-virus division of a small information technology security company based in Belarus, read an e-mail report explaining that a virus had infected a client's computer in Iran, and the virus caused the client's computer to continually reboot.[130] After obtaining a copy of the virus and sharing it among some colleagues, the men discovered that the virus was infecting Microsoft's Windows operating system, "using a vulnerability that had never been detected before."[131] Such a discovery is a substantial event; a vulnerability that the program's creator is unaware of and that has never before been detected is referred to as a "zero day."[132] Of the more than twelve million pieces of malware that antivirus researchers discover annually, fewer than a dozen utilize a zero-day vulnerability.[133] Windows' zero days can fetch as much as $100,000 on the black market likely because of their ability to be employed for a number of nefarious purposes.[134]

But the virus Ulasen and his colleagues was studying was remarkable in a number of other respects as well. For one, the virus spread in a way that had previously never been seen. By inserting a flash drive into a computer, the virus covertly uploaded two files—one, a piece of code that granted the virus complete control over the

---

129 *Id.*
130 Gross, *supra* note 4.
131 *Id.*
132 *Id.*
133 *See* Zetter, *supra* note 121.
134 *See* Gross, *supra* note 4.

computer, and second, a payload of heavily encrypted malicious code.[135]

Alarmingly, once the two components uploaded themselves from the flash drive, they hid themselves within the host computer.[136] Doing so is no simple task—the virus employed "a digital signature" to fool the host computer into believing the virus was a legitimate piece of software.[137] Digital signatures are analogous to passports; they serve as a proof of identity and legitimacy for software crossing from one computer to another.[138] In the past, malware writers have used fake, forged digital signatures to trick the target computer, but software security consultants have long suspected that sooner or later malware writers would jump to using genuine, stolen digital signatures instead.[139] The virus Ulasen and his colleagues had discovered was the first documented instance of a genuine, stolen digital signature.[140] Moreover, the digital signature had been stolen from one of the most trusted names in cyber-security—Realtek.[141] Thus, "the new virus Ulasen was looking at might as well have been carrying a cop's badge."[142]

Given the alarming sophistication of this virus, on July 5 Ulasen began alerting a number of authorities: first was Microsoft, to notify the company of the zero day vulnerability that the virus exploited; second was Realtek, to make the company aware of the stolen digital signature; finally, on July 12 Ulasen posted a report about the virus on a cyber-security message board.[143] Once alerted, internet authorities revoked the digital signature the virus was using.[144] But shockingly, on July 14 a new version of the virus appeared that used another genuine, stolen digital signature—this one from a different

---

135 *See id.*
136 *See id.*
137 *Id.*
138 *See id.*
139 *See id.*
140 *See id.*
141 *See id.*
142 *Id.*
143 *Id.*
144 *See* Zetter, *supra* note 121.

company.[145] This evidence strongly suggested that someone was actively helping the virus continue to avoid detection.[146]

Three days after Ulasen posted about the virus, a cyber-security blogger published a story about the virus—at this point dubbed "Stuxnet" by Microsoft using a combination of file names found in the malicious code.[147] As the news of Stuxnet spread, "antivirus companies around the world scrambled" to obtain copies of the malware for their own research purposes.[148] As the computer security industry worked to decrypt and deconstruct Stuxnet, more troubling information came to light. For one, it appeared that the virus first appeared around a year earlier—in June 2009—and its creator had updated and refined the virus numerous times, releasing at least three different versions before Ulasen's discovery in June 2010.[149]

Second, the geographical location of infected computers was anomalous. In the past, South Korea and the United States were overwhelmingly the epicenters of malware infections, given those countries' outsized number of Internet connections.[150] Of the 38,000 initial Stuxnet infections, approximately 22,000 were in Iran.[151] Indonesia placed a distant second with approximately 6,700 infections, and India with 3,700; the United States had fewer than 400 infections.[152] Third, researchers discovered that Stuxnet did not exploit a single zero day vulnerability in Windows, but instead *four* zero day vulnerabilities.[153] This "was unprecedented—one of the great technical blockbusters in malware history."[154]

The fourth anomaly was the virus's apparent target. Cyber-security experts deduced that "the virus was designed to target . . . an industrial control system made by the German conglomerate Siemens that was used to program controllers that drive motors, valves

---

145 *See* Gross, *supra* note 4.
146 *See id.*
147 *See* Zetter, *supra* note 121.
148 *Id.*
149 *Id.*
150 *See id.*
151 *See id.*
152 *See id.*
153 *See* Gross, *supra* note 4.
154 *Id.*

and switches in everything from food factories and automobile assembly lines to gas pipelines and water treatment plants."[155] Traditionally, computer viruses have been employed for financial gain, such as stealing credit card data, online banking information, and trade secrets.[156] Stuxnet's targeting of these industrial control systems—known as "programmable logic controllers," or PLCs—was odd because there was no obvious information to exploit for financial gain.[157] Stuxnet appeared to simply be stealing data from Siemens PLCs, and most experts were prepared to write Stuxnet off as an unusually sophisticated case of corporate espionage.[158]

Researchers from Symantec, one the world's largest engineers of computer security software, were dissatisfied with attributing such an advanced piece of malware to mere espionage and undertook a massive effort to discover Stuxnet's true purpose.[159] Throughout July 2010, a team of analysts and experts positioned across the globe[160] made the aforementioned discovery that Stuxnet's malicious payload would only spring into action once it detected that a host computer was running a piece of software that controls a Siemens PLC.[161]

Further, the Symantec engineers discovered that when Stuxnet found a host computer attached to a Siemens PLC, it would intercept the information exchanged between the host computer and the PLC.[162] Stuxnet would commandeer the PLC by injecting its own malicious code into the PLC, while simultaneously disabling any automated alarms the PLC would report back to the host computer; in effect, Stuxnet hid the rouge commands the virus was sending to the PLC from the host computer.[163] Thus, someone monitoring the PLC from the host computer would operate under the assumption that the PLC was functioning normally while in reality Stuxnet was serendipitously controlling the PLC.[164] In sum, Stuxnet worked

---

155 Zetter, *supra* note 121.
156 *See id.*
157 *Id.*
158 *See id.*
159 *See id.*
160 Gross, *supra* note 4.
161 Zetter, *supra* note 121.
162 *See id.*
163 *See id.*
164 *See id.*

"like a Hollywood heist film where jewelry thieves insert a looped video clip into a surveillance camera feed so that guards watching monitors see only a benign image instead of a live feed of the thieves in action."[165]

On August 6, 2010, Symantec published a blog post that laid out the company's findings regarding Stuxnet's true purpose.[166] But little immediate reaction followed because of a simple problem—most cyber-security experts knew very little about PLCs and what effect Stuxnet could have on them.[167]

Meanwhile in Germany, a man named Ralph Langner, who knew very little about cyber-security but quite a bit about PLCs, took up the case after reading Symantec's post.[168] "Langner knew that thousands of Siemens customers had a potentially silent killer on their system, and they were waiting for Symantec or Siemens to tell them what Stuxnet was doing to their industrial controllers."[169] Yet no word from Siemens or Symantec came, and thus Langner—with his primitive and self-taught knowledge of computers—delved into the virus's code himself.[170]

After three weeks of work, Langner and his small team came to a startling conclusion—Stuxnet was not aimed at all Siemens PLCs, as the corporate espionage theory would suggest; instead, the virus searched for a specific technical configuration—a single facility—and sought to infiltrate only it.[171] To Langner, the various clues pointed to a single conclusion: a well-funded organization, most likely a government with precise knowledge of its target, had written Stuxnet.[172] Langner explained his deduction as follows: "[t]o see

---

165 *Id.*

166 *See generally* Nicolas Falliere, *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*, SYMANTEC OFFICIAL BLOG (Aug. 6, 2010), http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

167 *See* Zetter, *supra* note 121.

168 *See id.*

169 *Id.*

170 *See id.*

171 *See id.*

172 *See id.*

that somebody built such [sic] sophisticated piece of malware—using four zero-day vulnerabilities, using two stolen certificates—to attack one single installation? That's unbelievable."[173]

While Stuxnet's exact target had not been identified, Langner had a hunch as to where the virus was aimed.[174] At one point, Langner announced to two colleagues, "[t]his is about taking out Bushehr," referring to an Iranian nuclear power plant that had been scheduled to go operational in August 2010 but had been delayed with little explanation.[175] Langner's colleagues were leery of his theory of state-sponsored cyber-terrorism that likely implicated the United States and Israel, but Langner remained undeterred.[176]

Eventually, Langner simply put his theory into the public; he posted on his blog his belief "that Stuxnet was the first literal cyberweapon," and it was aimed at the Iranian nuclear program at Bushehr.[177] On September 21, 2010, *The Christian Science Monitor* reported a story on Langner's theory;[178] the next day, another German computer expert went on the record to assert that Stuxnet's target was not Bushehr, but was instead Iran's Natanz uranium-enrichment facility.[179] On January 15, 2011, *The New York Times* accelerated the story, suggesting that Stuxnet was a covert United States intelligence project that began under President George W. Bush and hastened under President Barack Obama.[180]

As the rumors swirled online in response to Langner's theory, the engineers at Symantec continued to dismantle the virus's code, struggling to provide concrete evidence to corroborate one of the various theories.[181] The break came in November—Symantec had posted a request on its blog for anyone with expertise in critical infrastructure to contact Symantec, and a Dutch programmer wrote

---

173 *Id.*

174 *See id.*

175 *Id.*; *see also* Gross, *supra* note 4.

176 *See* Zetter, *supra* note 121.

177 Gross, *supra* note 4.

178 *Id.*; *see generally* Mark Clayton, *Stuxnet Malware Is 'Weapon' Out to Destroy . . . Iran's Bushehr Nuclear Plant?*, CHRISTIAN SCI. MONITOR (Sept. 21, 2010), http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

179 *See* Gross, *supra* note 4.

180 *See* Broad et al., *supra* note 120.

181 Gross, *supra* note 4.

back.[182] The Dutch programmer provided a critical piece of information that led Symantec to the ultimate resolution of Stuxnet's purpose.[183]

Using the Dutch programmer's tip, the Symantec engineers discovered that Stuxnet's target was not all PLCs but only a specific type of PLCs, called frequency converters.[184] "Frequency converters modulate the speed of motors and rotors in things like high-speed drills," so if you increase the frequency of the drive, then the rotor increases its spin.[185] Additional research into what type of machinery spun at the frequencies that Stuxnet modulated revealed a startling answer—the U.S. Nuclear Regulatory Commission regulates for export from the United States machines that spun at the frequencies Stuxnet targeted.[186] One Symantec engineer recalled the moment of enlightenment: "We realized, wait a second, these things, at this frequency, could be used for uranium enrichment."[187]

Thus, the engineers were able to corroborate Langner's theory and reveal what Stuxnet was doing when it injected its own malicious code into the PLCs: increasing the frequency that centrifuges spin.[188] In short, Stuxnet "was designed to send Iran's nuclear centrifuges spinning wildly out of control."[189] Symantec's discovery cemented the conclusion that Stuxnet was not intended for espionage but for causing physical damage.[190] Stuxnet "was the first time anyone had seen digital code in the wild being used to physically destroy something in the real world."[191] As Langner puts it, "Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept . . . . It is about destroying its targets with utmost determination in military style."[192]

Once the purpose of Stuxnet was discovered, the obvious next question was of attribution. In January 2011, *The New York Times*

---

182 *Id.*
183 Zetter, *supra* note 121.
184 *Id.*
185 *Id.*
186 *Id.*
187 *Id.*
188 *Id.*
189 Broad et al., *supra* note 120.
190 Zetter, *supra* note 121.
191 *Id.*
192 Broad et al., *supra* note 120.

published a lengthy story that alleged Israel's Dimona complex in the Negev desert—the heavily fortified center of Israel's never-acknowledged nuclear weapon program—doubled as a critical testing ground for Stuxnet.[193] The article further alleged that Stuxnet represented a "joint American and Israeli effort to undermine Iran's efforts to make a [nuclear] bomb of its own."[194] Within the Dimona's complex, the quoted experts asserted, Israel had spun the exact same type of nuclear centrifuges found at Natanz in an effort to test and refine the Stuxnet virus.[195] One American nuclear intelligence expert asserted, "To check out the worm, you have to know the machines . . . . The reason the worm has been effective is that the Israelis tried it out."[196]

One of the most difficult remaining questions surrounding Stuxnet was its degree of success. Given the opaqueness of the Iranian government, experts have differed on whether or not Stuxnet accomplished its ends.[197] A preliminary assessment paper for the Institute for Science and International Security asserted that Stuxnet's effectiveness is difficult to ascertain, given the uncertainty regarding both the virus's exact purpose and overall effect.[198] Given these limitations, the authors still asserted that if Stuxnet's aim was to destroy all of the centrifuges at Natanz, then Stuxnet failed; but if Stuxnet's goal was to destroy a limited number of centrifuges, thereby setting back the Iranian nuclear program while making detection of the virus difficult, then Stuxnet "may have succeeded, at least for a little while."[199] In sum, the data suggest that between late 2009 and early 2010, Iran faced significant difficulties with centrifuges at Natanz, decommissioning and replacing approximately 1,000 machines.[200]

---

193 *See id.*

194 *Id.*

195 *Id.*

196 *Id.*

197 *See* William Sweet, *Did Stuxnet Succeed?*, FOREIGN POL'Y BLOGS (Nov. 22, 2010), http://foreignpolicyblogs.com/2010/11/22/did-stuxnet-succeed/.

198 *See* DAVID ALBRIGHT, PAUL BRANNAN, & CHRISTINA WALROND, INST. FOR SCI. & INT'L SEC., DID STUXNET TAKE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? 1 (Dec. 22, 2010), http://www.isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.

199 *Id.*

200 *Id.*

The authors were careful to note that this level of replacement "exceeded expectations and occurred during an extended period of relatively poor centrifuge performance."[201]

B. *Implications for Critical Infrastructure*

While Stuxnet is fascinating in a myriad of respects—geopolitical and technological, to name a few—the virus also serves as a stark warning. Even in the wake of the Stuxnet virus, the critical infrastructure industry has shown little appetite for implementing measures that would remedy glaring vulnerabilities in its defenses. Organizations that own and operate critical infrastructure should adopt a WISP protocol in order to identify and mitigate the threats confronting them.

The problem that Stuxnet poses is that its target—PLCs—is ubiquitous in modern life.[202] The PLC is one of the most important modern manufacturing innovations.[203] By permitting manufacturers to automate industrial processes in real time, coupled with the ability to withstand extreme temperatures, electrical noise, and vibration, the PLC "changed the way we automate our factories and is still widely in use today."[204]

But before Stuxnet, few had reason to believe that PLCs were exploitable. Stuxnet represented "the first time anyone had seen digital code . . . being used to physically destroy something in the real world."[205] In testimony before the United States House of Representatives Committee on Energy and Commerce in July 2011, officials from the United States Department of Homeland Security (DHS) attested to Stuxnet representing a game changer:[206] "DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control

---

201 *Id.*

202 Alison Dunn, *The Father of Invention: Dick Morley Looks Back on the 40th Anniversary of the PLC*, MANUFACTURING AUTOMATION (Sept. 12, 2008), http://www.automationmag.com/features/the-father-of-invention-dick-morley-looks-back-on-the-40th-anniversary-of-the-plc.html.

203 *Id.*

204 *Id.*

205 Zetter, *supra* note 121.

206 *See Cybersecurity: An Overview of Risks to Critical Infrastructure: Hearing Before Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 112th Cong. (2011).

systems running a specific combination of software and hardware."[207] In the next breath, DHS officials warned that clones of Stuxnet could attack the country's power generation plants, water treatment facilities, and other critical infrastructure.[208] The officials asserted that the purpose of such an attack on critical infrastructure "would be to shut down or impair the infrastructure on which normal civilian life depends, diverting scarce resources, hurting civilian support for the war effort, and complicating military mobilization that depends on the civilian infrastructure."[209]

Yet the threat that Stuxnet clones pose for industrialized nations' critical infrastructure cuts two ways. On one hand, Stuxnet represents an opportunity for terrorists, hackers, criminals, or nation-states to infiltrate and damage another country's electrical, financial, gas, oil, water, and sewage systems. But on the other hand, Stuxnet's level of sophistication has left many industry leaders shrugging their shoulders, doubting that their systems are likely targets.

McAfee, another computer security giant, recently conducted a global survey of critical infrastructure companies to ascertain their level of cybersecurity and preparation against cyberattacks.[210] "Two-fifths of all respondents, and nearly half of those in the electric industry, said that they had found Stuxnet on their systems."[211] McAfee acknowledged that while Stuxnet was likely aimed at a single facility and was harmless to other sites, the widespread infection

---

[207] *Testimony of National Cybersecurity and Communications Integration Center Director Seán P. McGurk, National Protection and Programs Directorate, before the U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure"*, U.S. DEP'T OF HOMELAND SEC. (Apr. 14, 2011), https://www.dhs.gov/news/2011/04/14/testimony-national-cybersecurity-and-communications-integration-center-director-se%C3%A1n.

[208] Dan Goodin, *Stuxnet Clones May Target Critical US Systems, DHS Warns*, REGISTER (July 27, 2011, 12:15 AM), http://www.theregister.co.uk/2011/07/27/beware_of_stuxnet_clones/.

[209] STEWART BAKER, NATALIA FILIPIAK, & KATRINA TIMLIN, MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBERATTACKS 7 (Apr. 21, 2011), https://pdfsecret.com/download/in-the-dark-critical-industries-confront-cyberattacks_59f9ace0d64ab28ae25af226_pdf.

[210] *See id.*

[211] *Id.* at 9.

represents an utter failure of industry's cybersecurity measures.[212] Yet, "the discovery of Stuxnet on their systems did not seem to galvanize companies to action."[213] At least one expert attributes industry's inaction to governmental apathy, stating that "without clear government policy on the issue, individual ministries and companies are left to implement their own measures."[214]

Even more troubling, industry continues to willfully ignore the threat that a Stuxnet-like attack poses. Industry executives told McAfee with near unanimity that they remained more concerned about denial-of–service (DoS) attacks than about malware like Stuxnet.[215] A third of respondents to McAfee's global survey "declared that they were not at all confident or not very confident" in their ability to combat a DoS attack, but when prompted regarding malware designed for sabotage, "respondents expressed a similar lack of confidence only about 20 percent of the time."[216] A United States-based cybersecurity expert confirmed, "After Stuxnet, many people said, 'I don't have Siemens, I'm not nuclear—I could [sic] care less.'"[217] As McAfee noted in its published report, getting the critical infrastructure industry to perceive Stuxnet as a potential problem is a massive impediment to progress.[218]

Indeed, we have previously seen a very similar example of industry's inaction to the threat of a malware infiltration: the original wave of attacks on Microsoft's Windows in the 1990s. Microsoft was initially caught flat-footed when researchers and hackers first began exploiting vulnerabilities in Windows.[219] "It was only after several years of antagonism between [Microsoft headquarters] and the hackers ripping apart its software that Microsoft figured out how to work with hackers."[220] In the 1990s, researchers became so weary with Microsoft's inaction whenever the researchers would find a

---

212 *Id.*

213 *Id.*

214 *Id.*

215 *Id.* at 10.

216 *Id.*

217 *Id.*

218 *See id.* at 24.

219 Robert McMillan, *After Stuxnet, a Rush to Find Bugs in Industrial Systems*, TECHWORLD (Oct. 16, 2011), http://features.techworld.com/security/3311064/after-stuxnet-a-rush-to-find-bugs-in-industrial-systems/.

220 *Id.*

vulnerability, they simply began publishing technical details, thus forcing Microsoft to release a fix before the vulnerability could be exploited for nefarious ends.[221]

But continued antagonism between hackers and critical infrastructure is not tenable. Having this pattern repeat in the context of critical infrastructure is far more troublesome because "a security flaw could lead to a chemical spill or a widespread power blackout, and . . . it can take months to schedule and install [software fixes]."[222] One information-security expert with Boeing asserted that the infrastructure industry is "basically just 10 years behind the curve on security. It's like we're going back to the '90s."[223]

Finally, variations of the Stuxnet worm have been appearing nearly since it was first discovered. In October 2011, a new virus, dubbed "Duqu," which utilized large portions of Stuxnet's original source code, surfaced online.[224] According to Symantec, who initially posted a bulletin warning of the virus, Duqu's purpose is entirely different than Stuxnet.[225] Duqu's purpose is to gather intelligence data and assets from entities such as industrial control system manufacturers in order to more easily conduct a future attack against another third party.[226] The attackers are looking for information such as design documents that could help them mount a future attack on an industrial control facility.[227]

Similarly, in May 2012, a consortium of researchers unveiled their findings about a piece of malware related to Stuxnet, which they dubbed Flame.[228] Much like Stuxnet and Duqu, Flame is a com-

---

221 *See id.*

222 *Id.*

223 *Id.*

224 Shaun Waterman, *New Cyberweapon 'Duqu' Threatens Vital Infrastructure*, WASH. TIMES (Oct. 24, 2011), https://www.washingtontimes.com/news/2011/oct/24/new-cyberweapon-threatens-vital-infastructure/.

225 *See id.*

226 *See id.*

227 *W32.Duqu: The Precursor to the Next Stuxnet*, SYMANTEC: SECURITY RESPONSE (Oct. 24, 2011), http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

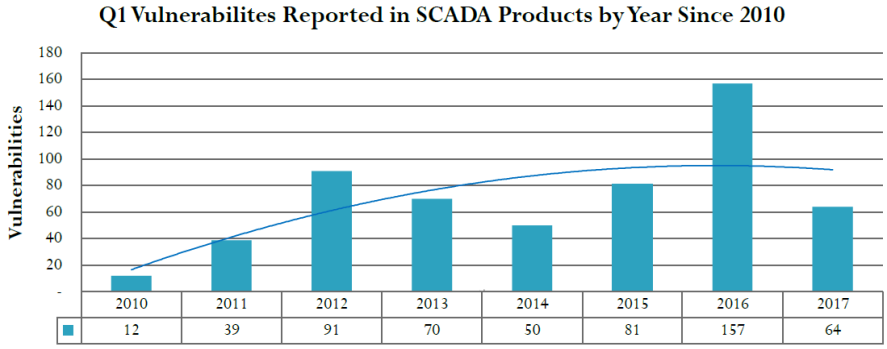
228 LAB. OF CRYPTOGRAPHY & SYS. SEC., BUDAPEST UNIV. OF TECH & ECON., SKYWIPER (A.K.A. FLAME A.K.A. FLAMER): A COMPLEX MALWARE FOR TARGETED ATTACKS 2 (2012), http://www.crysys.hu/skywiper/skywiper.pdf.

plex virus with a number of modular components that strongly suggest its use in a sophisticated, targeted attack.[229] Media reports later confirmed the United States' National Security Agency (NSA) developed all three strains of malware as part of the same Olympics Game operation.[230]

With Stuxnet's source code still widely available on the Internet, there is no telling who or what may utilize the original coding for new and more devastating attacks upon an industry that is moving too slowly in response to these warning signs.

Risk Based Security states that for 2017, SCADA products only accounted for 2% of all reported vulnerabilities.[231] In addition, "this decline in the number of vulnerabilities found in SCADA products seems to reflect the fact that researchers are no longer focusing on SCADA products rather than a significant improvement in SCADA product security."[232]

Exhibit 3
SCADA Vulnerabilities[233]



Source: Risk Based Security

---

229 *Id.* at 2–3.

230 Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST (June 19, 2012), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

231 *See* RISK BASED SEC., VULNERABILITY QUICKVIEW: 2017 VULNERABILITY TRENDS 12 (2018).

232 *Id.*

233 *Id.*

V. INTERNET OF THINGS

Continued rapid technological progress remains central to economic prosperity and social well-being, but it is also introducing potential new threats. The Internet of Things (IoT) is connecting billions of new devices to the Internet, but it also broadens the attack potential of cyber actors against networks and information.

Daniel R. Coats
Director of National Intelligence
May 11, 2017[234]

The term "Internet of Things" (IoT) describes "objects embedded with technologies such as microchips, sensors, and actuators that often use Internet Protocol and share data with other machines or software over communications networks."[235] Recall that the IoT

---

[234] *Statement for the Record: Hearing on Worldwide Threat Assessment of the US Intelligence Community Before the S. Select Comm. on Intelligence*, 115th Cong. 3 (2017) (statement of Daniel R. Coats, Director of National Intelligence).

[235] Katherine Britton, *Handling Privacy and Security in the Internet of Things*, 19 J. INTERNET L. 1, 3 (2016). *See also The Connected World: Examining the Internet of Things: Hearing Before the S. Comm. on Commerce, Sci., and Transp.* 114th Cong. 89–93 (2015) (statement of Adam D. Thierer, Senior Research Fellow, Mercatus Center, George Mason University); URS GASSER & JOHN PALFREY, BREAKING DOWN DIGITAL BARRIERS: WHEN AND HOW ICT INTEROPERABILITY DRIVES INNOVATION 4 (2007), https://cyber.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf; ELLEN P. GOODMAN, THE ASPEN INST., THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS 2–4 (2015), http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf; Eric Barbry, *The Internet of Things, Legal Aspects: What Will Change (Everything) . . .* , 87 DIGIWORLD ECON. J. 83, 86–87 (2012); Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641–42 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, & Consent*, 93 TEX. L. REV. 85, 88–89 (2014); Gilles Privat, *Extending the Internet of Things*, 87 DIGIWORLD ECON. J. 101, 106 (2012); Jaclyn Selby, *Anyone's Game: Economic and Policy Implications of the Internet of Things as a Market for Services*, 87 DIGIWORLD ECON. J. 21, 22 (2012); Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things"*, 2017 U. ILL. L. REV. 415, 421 (2017); T.H.A. Wisman, *Purpose and Function Creep by Design: Transforming the Face of Surveillance Through the Internet of Things*, 4 EUR. J.L. & TECH. 1, 1 (2013); Daniela Rus, *The Robots Are Coming: How Technological Breakthroughs Will Transform Everyday Life*, 94 FOREIGN AFF. 1, 2 (2015); Paul Kominers, *Interoperability Case*

global market spend is estimated to "grow from $591.7 billion in 2014 to $1.3 trillion in 2019 with a compound annual growth rate of 17%. The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019."[236]

A. *The Promise of the Internet of Things*

The IoT makes possible a wide assortment of truly wonderful benefits for daily life. The IoT is "in your home, in your car and phone, and, increasingly, on your body. It's connecting citizens to their cities, linking patients to health services, bringing companies in closer touch with their customers and capturing our imaginations."[237] Although most Internet data "currently takes the form of text files, messages, audio, photographs, and video files, the IoT grabs new and different data, it combines data in different ways and it allows humans and machines to gain broader and deeper insights."[238]

The IoT "quite literally means 'things' or 'objects' that connect to the Internet—and each other."[239] Examples are everywhere and include airplane engines, e-books, computers, Fitbit devices, home heating and air conditioning systems, home security cameras, and smartphones.

Study: Internet of Things (IoT) 3 (The Berkman Ctr. for Internet & Soc'y, Harvard Univ., Research Publication No. 2012-10, 2012), http://ssrn.com/abstract=2046984; Paul Kominers, *Interoperability Case Study: The Smart Grid* 2 (The Berkman Ctr. for Internet & Soc'y, Harvard Univ., Research Publication No. 2012-6, 2012), http://ssrn.com/abstract=2031113; William H. Dutton, The Internet of Things 4 (June 20, 2013) (unpublished manuscript), http://ssrn.com/abstract=2324902; William Dutton, et al., A Roadmap for Interdisciplinary Research on the Internet of Things: Social Sciences 2 (Jan. 5, 2013) (unpublished manuscript), http://ssrn.com/abstract=1033226; John Gudgel, Objects of Concern?: Risks, Rewards and Regulation in the "Internet of Things," 3–8 (Apr. 30, 2014) (unpublished manuscript), http://ssrn.com/abstract=2430780; Adam D. Thierer & Andrea Castillo, *Projecting the Growth and Economic Impact of the Internet of Things*, MERCATUS CTR. (June 15, 2015), https://www.mercatus.org/system/files/IoT-EP-v3.pdf.

236 VERIZON, *supra* note 5, at 3.

237 *Id.*

238 GREENGARD, *supra* note 74, at 19.

239 *Id.* at 15.

> Each of these devices or things has a unique identification number (UID) and an Internet Protocol (IP) address. These objects connect via cords, wires and wireless technology, including satellites, cellular networks, Wi-Fi, and Bluetooth. They use built-in electronic circuitry as well as radio frequency identification (RFID) or near-field communication (NFC) capabilities that are added later via chips and tags. Regardless of the exact approach, the IoT involves the movement of data to enable processes from across the room or somewhere on the other side of the world.[240]

It is the IoT that enables "epidemiologists to track the spread of viruses in near real time. A grocery store can analyze how people shop and the products they view and buy as an individual walks through the store . . . . A pharmaceutical firm can understand consumption patterns in real time."[241] Because of the IoT, "a city can crunch data from sensors and other systems to better manage congestion, waste management, utilities, natural resources, and much more . . . . The technology brings intelligence and a far greater level of insight and understanding to a vast array of physical and virtual systems."[242]

B. *Unintended Consequences*

The future of the IoT is not all positive. Unintended consequences include the likelihood of "new types of crime, weapons and warfare. It could also create significant political and social problems by, among other things, contributing to a growing disconnect between people. It will certainly cause society to more closely examine the notion of privacy and security."[243] Indeed, the information-silo

---

240 *Id.*
241 *Id.* at 14.
242 *Id.*
243 *Id.* at xv.

or information-bubble phenomenon presents a societal and management governance threat.[244]

Akamai observed, "The rapid proliferation of IoT devices, primarily in the home environment, adds a . . . layer of problems for network defenders. The creation of new features to distinguish one's products in the market is always a driving factor for manufacturers."[245] This is a costly societal problem because "[t]here are far too many organizations that consider security to be at the bottom of their list of priorities, if they consider it at all."[246] For example, Korean appliance manufacturer LG recently attended the Las Vegas Consumer Electronics Show, "where not only was an Internet refrigerator announced, but LG stated that every device it sells in the near future will have Internet-connected capabilities. Regardless of LG's success at securing these devices, they are establishing a new standard feature set, which low-end competitors will move to emulate."[247] Akamai raises the question, "Does every home need a refrigerator that not only takes pictures of its own contents, but also has a built-in web browser on the front? The market seems to think they do, but the security implications are troublesome."[248]

Instances of hackers infiltrating automobiles, baby monitors, and video cameras are reported in the popular media.[249] With a goal of exposing vulnerabilities to manufacturers so that they may improve their products, so-called white-hat hackers have found and reported code weaknesses in IoT-connected medical devices, "including insulin pumps, ventilators, and defibrillators."[250]

FTC Chairwoman Edith Ramirez stated, "We have seen an explosion of surveillance technologies, such as drones and mobile device tracking sensors in retail stores. We have moved from an ecosystem where companies track consumers across websites to one

---

244 *See* Lawrence J. Trautman, *Governing Risk and the Information Silo Problem: Engineering a Systemic Cultural and Communications Solution for Cyber* 6–7 (Mar. 19, 2017) (unpublished manuscript), https://ssrn.com/abstract=2925352.

245 AKAMAI TECHS., STATE OF THE INTERNET / SECURITY Q4 2016 REPORT 6 (Martin McKeay ed., 2016), https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf.

246 *Id.*

247 *Id.*

248 *Id.*

249 *See* GREENGARD, *supra* note 74, at 24.

250 *Id.*

where companies track us across apps and even across devices."[251] She further warned, "And now, many consumer devices and appliances—from your [F]itbit to your fridge to your thermostat—are silently talking to one another, collecting data, and transmitting that information to various third parties."[252] Some may be surprised to learn that "even the once private act of reading is generating data about us, as e-book companies track not just what we read, but also how we read—where we start, what passages we skim, reread, or highlight, and whether we actually finish the books we begin."[253]

1. UNDERLYING TECHNOLOGY

The genesis of the term "Internet of Things" is credited to technology pioneer Kevin Ashton, who reportedly incorporated the term in a presentation he made to Proctor & Gamble (P&G) in 1999.[254] Ashton's idea was to link the Internet with Radio Frequency Identification (RFID) technology and to interest retail giants such as P&G.[255] Today's RFID tags, "can be produced for under a penny and are capable of performing real-time, constant data exchange and can be read by scanners."[256] It wasn't until the early 2000s that technological advances provided a platform for achieving the true potential of Internet-connected devices.[257]

2. GROWTH AND IMPORTANCE OF MOBILE

A single incident responsible for catapulting the IoT into exponential growth is difficult to isolate. However, introduction of the Apple iPhone in 2007:

---

[251] Edith Ramirez, Chairwoman, Fed. Trade Comm'n., Keynote Address at the Technology Policy Institute Aspen Forum (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf.

[252] *Id.*

[253] *Id.*

[254] *See* Shackelford et al., *supra* note 235, at 421 (citing Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), www.rfidjournal.com/articles/view?4986).

[255] *Id.*

[256] Britton, *supra* note 235, at 3.

[257] *See* GREENGARD, *supra* note 74, at xii.

> was a crystallizing event. It put smartphones into the hands of the masses. It put real-time . . . communication on the map . . . . Consider: In January 2008, Apple had sold approximately 3.7 million units. By June 2014, the number had topped 500 million. Today, the total number of smartphones in use worldwide is somewhere in the vicinity of 1.9 billion. By 2019, Sweden telecom firm Ericsson estimates the number will exceed 5.6 billion.[258]

The explosive growth since 2010 of dynamic IoT devices is "based on insights gleaned from the processing of real-time information and historical data with minimum human interaction," and results from three main catalysts.[259] When combined, three factors provided a perfect environment of smart and interconnected devices that nurtured the creation of the IoT:

> First, the widespread availability of broadband Internet provided high speed network connectivity that enabled devices to communicate with each other over a wireless network across large parts of the developed world. Second, enhanced computational capabilities enabled the real-time analysis of large amounts of unstructured data.
>
> Third, the decreasing cost of sensors allowed manufacturers to add small wireless chips to any device for a minor incremental cost.[260]

Application of RFID technology is much more than just a tool for maximizing profits and reducing costs. Samuel Greengard observed that RFID:

> builds a bridge between the physical world and the virtual world. By attaching a small tag to an object (or installing a chip into a device)—either a tiny passive transponder using electromagnetic radiation or a

---

258 *Id.* at xii–xiii.

259 *See* Shackelford et al., *supra* note 235, at 421–22.

260 *Id.* at 422 (footnotes omitted).

> battery powered passive or active tag that relies on UHF radio waves—and setting up an RFID reader, anything and everything can be connected to the Internet. Today RFID technology is used for toll collections, contactless payment systems, tracking animals, managing baggage at airports, embedding data in passports, following runners in [sic] marathons, and tracking golfballs via a smartphone app.[261]

3. INDUSTRIAL INTERNET

Samuel Greengard describes the Industrial Internet as revolving "around machines equipped with sensors, thus making them 'smart.' These devices often serve as the plumbing or IT foundation for the IoT."[262] It is the connectivity to sensor technology devices and miniaturization that is at the very heart of the Industrial Internet. These newly available data points and systems connectivity make possible, "things as diverse as geolocation and GPS devices, bar code scanners, thermometers, barometers, humidity gauges, vibration sensors, pressure sensors, gyroscopes, magnetometers, cameras, audio and video monitors, accelerometers, motion sensors, radar, sonar, and lidar" (used by Google to operate its driverless car).[263] Key capabilities made possible by the Industrial Internet include: location awareness;[264] enhanced situational awareness;[265] sensor-based decision analytics;[266] automation and controls;[267] and a connected military.[268]

A series of competing protocols and communications technologies are involved in the contemporary IoT ecosystem. These technologies include: actuator networks; machine-to-machine (M2M) communications; near-field communications (NFC); RFID; and

---

261 *See* GREENGARD, *supra* note 74, at 33.
262 *Id.* at 17.
263 *Id.* at 57–58.
264 *See id.* at 60–64.
265 *See id.* at 64–67.
266 *See id.* at 67–69.
267 *See id.* at 69–72.
268 *See id.* at 72–74.

wireless sensor devices and networks.[269] Katherine Britton observes:

> NFC evolved from RFID and is a short-range, low-power wireless way to transfer small amounts of data between devices; NFC technology is built into 20 percent of mobile phones and most commonly is used for mobile payment services such as Google Wallet. M2M transmissions refer to direct communications between machines such as a microchip and a microchip scanner, a wearable and a third-party application (app), or a wearable and a monitoring hub. When machines communicate directly with other machines, a device collects information through a sensor that can then use a radio transmitter to send the data over a wired or wireless network. M2M transmissions share information without any special configuration or other setup requirements. Cellular and mobile data transmission standards such as LTE, 4G, GSM, and CDMA will connect devices to the mobile phone network. Larger "things" will be able to communicate via fixed wire lines such as Ethernet and optical fiber. Most connections likely will take place via wireless networks with chips embedded into "things" using standards such as Wi-Fi, Bluetooth, ZigBee, Z-Wave, NFC, and RFID in order to communicate. The number of installed M2M connections continues to grow due to the declining cost of sensors and increased connectivity capabilities and data processing power.[270]

4. IoT AND HEALTH

The potential benefits and implications of IoT in medicine delivery and health care are enormous. Greengard observes that RFID sensors or other "devices implanted in the human body or worn on the body could gather data and use the IoT to transmit specific in-

---

269 Britton, *supra* note 235, at 3.

270 *Id.* at 3–4.

formation about blood pressure, blood sugar, heartbeat and other vitals while also monitoring medication dosage."[271] Immediately upon detecting a problem while monitoring elderly patients, nanobots could notify a physician.[272] Greengard provides the example of Portland's Oregon Health Sciences University (OHSU) as a healthcare real-time location system (RTLS).[273] Accordingly:

> health and research institution tags assets ranging from infusion pumps to crutches so that they are easy to locate. In addition they are able to track performance data related to the device. This approach not only saves time that would otherwise be spent hunting down equipment, it helps ensure that devices are in working order. OHSU is now looking into tagging patients and clinicians to better understand where they spend time, how they move around within the facility, and how long patients wait in a room before a clinician arrives.[274]

5. VALUE PROPOSITION

The profound healthcare benefits cited above raise the very real subjective issue on how to appropriately place a monetary value on life. Any such inquiry is far beyond the scope of this article. However, it is apparent that sensor technologies and the Industrial Internet present a potentially exponential technological benefit, perhaps spawning "economic activity measuring in the tens of trillions of dollars."[275] As Greengard observed, "[e]ven a 1 percent reduction in fuel costs or a similar improvement in capital expenditures of system inefficiency could produce savings in the tens of billions or hundreds of billions of dollars."[276]

---

271 GREENGARD, *supra* note 74, at 21.
272 *See id.*
273 *Id*. at 62–63.
274 *Id.*
275 *Id.* at 60.
276 *Id.*

6. IoT Exploitable Security Flaws

In his prepared remarks before the Senate Select Committee on Intelligence in 2017, Director of National Intelligence Daniel R. Coats observed:

> The widespread incorporation of "smart" devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.[277]

By mid-2016, numerous security flaws in IoT devices were being exploited, as demonstrated by the Mirai botnet attacks.

7. Mirai Botnet Attacks

Akamai began tracking a strain of malware during June 2016 that targets IoT devices and home Internet routers.[278] Soon thereafter, this malware, under the name Mirai, spread worldwide.[279] Akamai observed that "Mirai [is] truly exceptional i[n] its use of IoT devices and several capabilities that aren't often seen in botnets: specifically, Generic Routing Encapsulation (GRE) based attacks, varying levels of attack traffic customization, and telnet scanning. In

---

[277] *Statement for the Record: Hearing on Worldwide Threat Assessment of the US Intelligence Community Before the S. Select Comm. on Intelligence*, 115th Cong. 4 (2017) (statement of Daniel R. Coats, Director of National Intelligence).

[278] *See* Akamai Techs., State of the Internet / Security Q3 2016 Report 6 (Martin McKeay & Amanda Fakhreddine eds., 2016), https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf.

[279] *Id.*

addition, it generates its attacks directly . . . ."[280] Akamai predicted, "Due to the public release of the source code . . . we're likely to see new, more-capable variants of Mirai in the near future."[281] Moreover, Akamai found:

> Mirai is a botnet that would not exist if more networks practiced basic hygiene, such as blocking insecure protocols by default. This is not new—we've seen similar network hygiene issues as the source of infection in the Brobot attacks of 2011 and 2012. The botnet spreads like a worm, using telnet and more than 60 default username and password combinations to scan the Internet for additional systems to infect. The majority of these systems appear to be Digital Video Recorders (DVRs), IP-enabled surveillance cameras, and consumer routers. Once a system is infected, it connects to the command and control (C2) structure of the botnet, then continues scanning for other vulnerable systems while waiting for attack commands.[282]

8. KREBS ON SECURITY ATTACKS

In its Q3 2016 Internet security report, Akamai noted that the two highest volume attacks seen as of that date on the Prolexic network consisted of attacks on sites used by security blogger Brian Krebbs.[283]

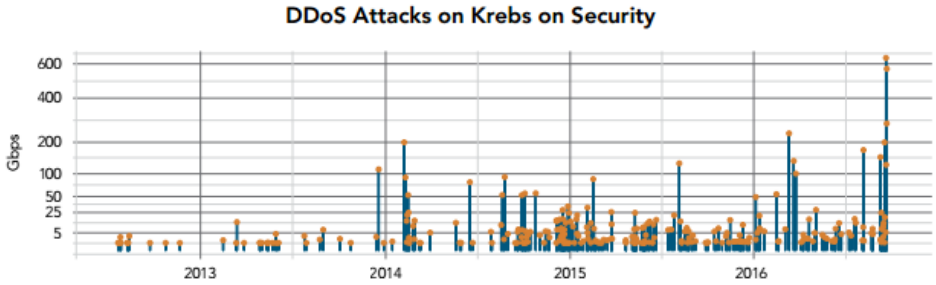
Krebs is a security blogger who has been the target of extensive large-scale DDoS attacks in response to his reporting.[284] According to Akamai, Krebs was the target of 269 attacks between 2012 and 2016.[285] Exhibit 4 details the size and timing of the DDoS attacks on Krebs on Security during this period, and Akamai noted that a series of attacks in September 2016 were the largest DDoS attacks

---

280 *Id.* at 15.
281 *Id.*
282 *Id.* at 15–16.
283 *Id.* at 13.
284 *Id.* at 13–14.
285 *Id.* at 14.

Akamai has defended against.[286] Akamai explained that an "observant reader can probably correlate clumps of attacks to specific stories covered by Krebs," and also opined that "[r]eporting on the dark side of cybersecurity draws attention from people and organizations who are not afraid of using DDoS attacks to silence their detractors."[287]

Exhibit 4
All Attacks Mitigated for krebsonsecurity.com while on the Routed Platform[288]



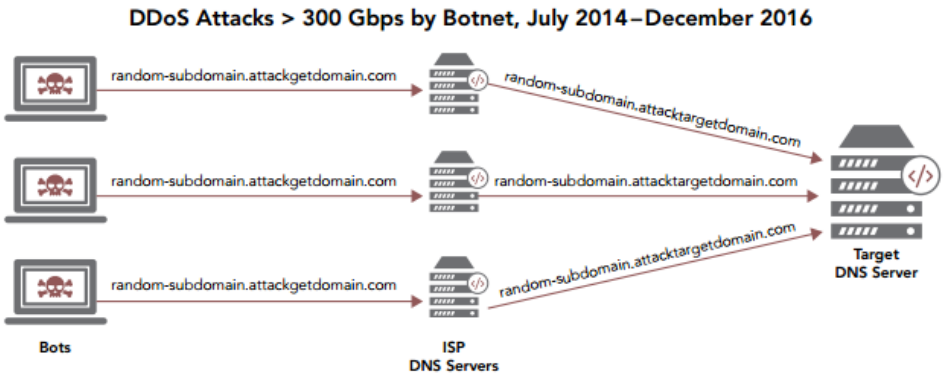
Source: Akamai

Before 2016, "the largest DDoS attacks were in the range of 100 Gbps, growing to 300 Gbps in first half of 2016, and finally into the 500–600 Gbps range in the third quarter."[289] Exhibit 5 depicts how the Mirai botnet produces a specific Domain Name System (DNS) query flood. Akamai explained that "this dns query flood can potentially cause more damage than current dns reflection attacks. If a targeted dns server is unprepared for a sustained flood of queries with high packet rates, dns Water Torture can lead to a denial of service for legitimate users."[290]

---

286 *Id.*
287 *Id.* at 14.
288 *Id.* at 14.
289 AKAMAI TECHS., *supra* note 45, at 17.
290 *Id.* at 8.

Exhibit 5
Mirai DNS Attack Queries Are Sent from Bots to their Local DNS Servers and go on to the Target Authoritative DNS Servers[291]



Source: Akamai

By the first quarter 2017, Akamai detected additional disruptive Mirai attacks and observed that "[t]he botnets' capabilities quickly moved into a stage where contention for Internet of Things (IoT) devices reduced the size of attacks considerably. While many of the largest DDoS attacks observed this quarter were still based on Mirai-derived botnets, they were not as large as the initial attacks."[292] The Marai case study reveals that to be effective, attacks need not be particularly big. Akamai stated, "If we consider that many businesses lease uplinks to the Internet in the range of 1–10 Gbps, any attack exceeding 10 Gbps could be 'big enough' and more than capable of taking the average unprotected business offline."[293] In addition, Akamai warned:

> the effects of IoT are not to be underestimated, and the IoT ecosystem has drawn the attention of a wider audience. A recent example is malware that compromises Internet-enabled toasters to mine Bitcoins, an effort that appears to have been an ineffective proof of concept. Another trend is represented by the

291 *Id.*
292 *Id.* at "Letter from the Editor."
293 *Id.* at 2.

> BrickerBot botnet, which attacks systems exposed directly to the Internet with default Telnet passwords apparently in an attempt to prevent their use by the Mirai botnet. If this botnet is unable to disconnect the target device from the Internet, it corrupts the configuration, permanently bricking the devices. Neither of these examples are major threats, but they do show a significant increase in attention from both the hacker and security communities.
>
> There is one factor that seems to be affecting the DDoS landscape as a whole: law enforcement. Early attacks by the Mirai botnets appear to have been triggered by the announcement of the arrests of two teens in Israel who were responsible for the vDos botnet—a DDoS-for-hire tool that netted them hundreds of thousands of dollars. More recently, Europol coordinated the arrest of 34 individuals across 13 countries as part of an effort called Operation Tarpit. Operations like Tarpit target the largest services responsible for DDoS attacks directed at banks, gaming companies, and retailers. This can have a significant effect in reducing the number of attacks on these organizations.[294]

Efforts to combat these threats are complicated by the fact that most of these botnets are discrete code compositions, making for an expanding universe of numerous "Mirai-derived botnets using similar software, each a small fragment and distinct entity . . . . One concern is that a unified command and control (C2) structure could emerge . . . . [and] such a super botnet could generate a DDoS attack of two Tbps in the near future."[295] Ultimately, "[i]f these networks gain unfettered Internet access, the devices could be capable of emitting 20 times more attack traffic than we've seen to date."[296]

Europol is credited with coordinating global efforts among the international security community to combat Mirai IoT-based botnets

---

294 *Id.*
295 *Id.* at 18.
296 *Id.*

including Mirai.[297] Akamai cautioned how myopic it is to consider Mirai as the only threat.[298] "With the release of the source code, any aspect of Mirai could be incorporated into other botnets. Even without adding Mirai's capabilities, there is evidence that botnet families like BillGates, elknot, and XOR are mutating to take advantage of the changing landscape."[299] As to the future, Akamai urges the importance of recognizing that DDoS and IoT's other threats "are just one aspect of the threat landscape . . . . Organizations may monitor the login page logs of their sites, but are they watching the traffic for their [application programming interfaces (APIs)]? Site-to-site and business-to-business APIs may be a bigger target than most realize."[300]

9. FTC AND CONSUMER PROTECTION

The FTC has begun to address IoT matters that impact consumers in the United States.[301] On August 22, 2016, FTC Chairwoman Ramirez discussed the important role of the FTC "in empowering consumers and ensuring they have control over their personal information."[302] Chairwoman Ramirez argued that control may be achieved by:

> (1) conducting research to ensure that our policy-making efforts appropriately address privacy and security risks as the marketplace evolves; (2) using our law enforcement authority to ensure that consumers' choices are honored and that companies safeguard the consumer data they collect; and (3) helping spur innovation in the creation of tools that help consumers express choices.[303]

---

297 *See id.*

298 *Id.*

299 *Id.*

300 *Id.*

301 *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.

302 Ramirez, s*upra* note 251, at 10.

303 *Id.*

One example of such law enforcement authority is the FTC's 2017 agreement with VIZIO to settle charges the consumer electronics company collected viewing histories on 11 million smart televisions without consent from users.[304] Other FTC actions implicating consumer protection have addressed issues such as artificial intelligence;[305] blockchain technology;[306] and computer routers and cameras.[307] For example, the FTC brought an action during 2016 against ASUS, a manufacturer of wireless routers.[308] In discussing the critical importance of subjecting IoT devices to pre-launch security testing, Chairwoman Ramirez observed that in the ASUS matter, "we alleged that the company's failure to test its Internet-connected routers prior to launch contributed to several security breaches. We

---

[304] *See* Press Release, Fed. Trade Comm'n, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[305] *See* Press Release, Fed. Trade Comm'n, FTC to Host FinTech Forum on March 9 on Artificial Intelligence and Blockchain Technology (Mar. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-host-fintech-forum-march-9-artificial-intelligence-blockchain.

[306] *See* Press Release, Fed. Trade Comm'n, FTC to Host FinTech Forum on Artificial Intelligence and Blockchain March 9 (Jan. 13, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-host-fintech-forum-blockchain-artificial-intelligence-march-9.

[307] *See* Press Release, Fed. Trade Comm'n, D-Link Case Alleges Inadequate Internet of Things Security Practices (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security (implicating D-Link's routers, IP cameras, baby monitors and other products designed to integrate consumers' home networks).

[308] *See* Ramirez, *supra* note 251, at 12.

charged that ASUS' actions were both deceptive and unfair, in violation of Section 5."[309] Other subject areas of focus for the FTC include connected cars;[310] consumer demographics;[311] consumer scams;[312] crowdfunding;[313] data breach;[314] and data security.[315] An example of data security enforcement may be found in the FTC's 2016 action taken against large advertising network InMobi.[316] The

---

[309] *Id.* (citing Press Release, Fed. Trade Comm'n, ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk (Feb. 23, 2016), https://www.ftc.gov/news-events/pressreleases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put).

[310] *See* Press Release, Fed. Trade Comm'n, FTC Extends Deadline for Comments on Privacy, Security Issues to Be Examined as Part of Connected Cars Workshop (Apr. 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-extends-deadline-comments-privacy-security-issues-be-examined.

[311] *See* Press Release, Fed. Trade Comm'n, FTC Workshop Will Examine Changing Consumer Demographics (Nov. 8, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-workshop-will-examine-changing-consumer-demographics.

[312] *See* Press Release, Fed. Trade Comm'n, FTC Puts an End to Data Broker Operation that Helped Scam More than $7 Million from Consumers' Accounts (Nov. 30, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million; Press Release, Fed. Trade Comm'n, FTC Presents Criminal Liaison Unit Award to Fraud and Cybercrime Unit of the U.S. Attorney's Office for the Southern District of New York (Oct. 19, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/ftc-presents-criminal-liaison-unit-award-fraud-cybercrime-unit-us.

[313] *See* Press Release, Fed. Trade Comm'n, FTC Announces Agenda, Panelists for Oct. 26 FinTech Forum on Peer-to-peer Payments and Crowdfunding (Oct. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/ftc-announces-agenda-panelists-oct-26-fintech-forum-peer-peer.

[314] *See* Press Release, Fed. Trade Comm'n, Operators of AshleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting; Press Release, Fed. Trade Comm'n, What to Do When You Suspect a Data Breach: FTC Issues Video and Guide for Businesses (Oct. 25, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/what-do-when-you-suspect-data-breach-ftc-issues-video-guide.

[315] *See* Press Release, Fed. Trade Comm'n, FTC to Host Data Security Conference in Chicago June 15 (Apr. 7, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-host-data-security-conference-chicago-june-15.

[316] *See* Ramirez, *supra* note 251, at 11 (citing Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22,

FTC charged InMobi with violations of Section 5 of the FTC Act, based upon InMobi's deceptive activities.[317] Chairwoman Ramirez explained,

> InMobi offered app developers software code to embed in their apps to enable them to serve targeted advertising, including advertising based on geolocation. It represented that its software would track consumers' locations only when consumers had granted access to that information. The FTC alleged that, in actuality, InMobi had used consumers' geolocation information, which it was able to infer, to target ads, even when consumers had not granted geolocation permission.[318]

As IoT devices proliferate and as digital threats become increasingly sophisticated, the FTC's policing of companies' digital privacy practices is becoming increasingly pervasive. The FTC's areas of focus have become extremely broad and include a vast array of

---

2016), https://www.ftc.gov/newsevents/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked).

317 *Id.*

318 *Id.*

topics like data security and small businesses;[319] digital advertising;[320] drones;[321] e-commerce;[322] how electricity generation facilities connect to the transmission grid;[323] FinTech (artificial intelligence and blockchain);[324] health apps;[325] home devices;[326] identity

---

[319] *See* Press Release, Fed. Trade Comm'n, FTC Testifies Before House Committee About Data Security and Small Businesses (Mar. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-testifies-house-committee-about-data-security-small.

[320] *See* Press Release, Fed. Trade Comm'n, Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices (Dec. 20, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively.

[321] *See* Press Release, Fed. Trade Comm'n, FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues (Mar. 31, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

[322] *See* Press Release, Fed. Trade Comm'n, FTC Welcomes Revised OECD Guidelines for E-commerce (Apr. 4, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-welcomes-revised-oecd-guidelines-e-commerce.

[323] *See* Federal Trade Commission, Comment on Federal Energy Regulatory Commission's Proposed Rule Concerning "Reform of Generator Interconnection Procedures and Agreements" (Apr. 10, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commission-federal-energy-regulatory-commission-concerning-reform/v170004_ferc_interconnection_ftc_staff_comment.pdf.

[324] *See* Press Release, Fed. Trade Comm'n, FTC Announces Agenda for March 9 FinTech Forum on Artificial Intelligence and Blockchain Technology (Feb. 27, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/ftc-announces-agenda-march-9-fintech-forum-artificial.

[325] *See* Press Release, Fed. Trade Comm'n, FTC Releases New Guidance for Developers of Mobile Health Apps (Apr. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps.

[326] *See* Press Release, Fed. Trade Comm'n, *supra* note 301.

theft;[327] mobile devices;[328] online tracking of consumers;[329] peer-to-peer payment systems;[330] personal information scams;[331] privacy and consumer protection;[332] ransomware;[333] sharing economy platforms;[334] smart TV;[335] software developer risks;[336] software security

---

[327] *See* Press Release, Fed. Trade Comm'n, Identity Theft: Planning for the Future (May 24, 2017), https://www.ftc.gov/news-events/events-calendar/2017/05/planning-future-conference-about-identity-theft (observing that during 2014, 17.6 million individuals—7% of all U.S. residents age 16 and older—were victims of one or more incidents of identity theft).

[328] *See* Press Release, Fed. Trade Comm'n, FTC to Study Mobile Device Industry's Security Update Practices (May 9, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[329] *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Consent Order with Online Company Charges with Deceptively Tracking Consumers Online and Through Mobile Devices (Apr. 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-consent-order-online-company-charged.

[330] *See* Press Release, Fed. Trade Comm'n, *supra* note 310.

[331] *See* Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

[332] *See* Press Release, Fed. Trade Comm'n, How to Participate in FTC's Second PrivacyCon (Jan. 11, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/how-participate-ftcs-second-privacycon.

[333] *See* Press Release, Fed. Trade Comm'n, FTC Offers Advice on How to Avoid and Respond to Ransomware Attacks (Nov. 10, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-offers-advice-how-avoid-respond-ransomware-attacks.

[334] *See* FED. TRADE COMM'N, THE "SHARING" ECONOMY: ISSUES FACING PLATFORMS, PARTICIPANTS & REGULATORS 1–9 (2016), https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf.

[335] *See* Lesley Fair, *Ransomware, Smart TV, Drones—Oh, My!*, FED. TRADE COMMISSION: BUS. BLOG (Mar. 31, 2016, 11:04 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/03/ransomware-smart-tv-drones-oh-my.

[336] *See* Press Release, Fed. Trade Comm'n, FTC Issues Warning Letters to App Developers Using 'Silverpush' Code (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

issues;[337] technology used to track consumers across multiple Internet-connected devices;[338] and telecommunications regulation.[339]

VI. EXPOSURE OF U.S. GOVERNMENT CYBER TOOLS

Not even the highest echelons of government military-grade cyber secrets are safe. Over the past two years, multiple parties have come into possession of cyber weapons developed and used by the U.S. government. Beginning in August 2016, a hacker collective known only as "the Shadow Brokers" began releasing and auctioning off a set of cyber weapons belonging to the NSA's highly secretive Office of Tailored Access Operations (TAO).[340] Tools released by the Shadow Brokers in April 2017 have been implicated in the massive ransomware threat known as WannaCry.[341] In March 2017, Wikileaks released a huge trove of partially redacted hacking tools that the organization attributed to the Central Intelligence Agency (CIA).[342]

---

337 *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order in Oracle Java Security Case (Mar. 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-approves-final-order-oracle-java-security-case.

338 *See* Press Release, Fed. Trade Comm'n., FTC Releases New Report on Cross-Device Tracking (Jan. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-releases-new-report-cross-device-tracking.

339 *See* Press Release, Fed. Trade Comm'n, FTC Staff Provides Response to NTIA Request for Comment on Internet of Things (June 3, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/ftc-staff-provides-response-ntia-request-comment-internet-things.

340 *See* Joseph Menn, *Russian Researchers Expose Breakthrough U.S. Spying Program*, REUTERS (Feb. 16, 2015, 2:43 PM), http://www.reuters.com/article/us-usa-cyberspying-idUSKBN0LK1QV20150216; David E. Sanger, *'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?*, N.Y. TIMES (Aug. 16, 2016), https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html.

341 *See* Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html.

342 Greg Miller & Ellen Nakashima, *WikiLeaks Says It Has Obtained Trove of CIA Hacking Tools*, WASH. POST (Mar. 7, 2017), https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html.

A. *NSA and the Shadow Brokers*

In August 2016, the Shadow Brokers announced a putative auction of a series of cyber tools that the group claimed had been stolen from the "Equations Group," a highly advanced hacking group that has been connected with TAO.[343] The Shadow Brokers released a number of leaks during 2016, including tools aimed at exploiting firewalls and network infrastructure engineered by companies that include Cisco, Juniper, Fortinet, and Huawei, a Chinese company.[344]

At the same time, the group also released another cache of encrypted files, claiming they would provide the password to this cache to the winner of a Bitcoin auction.[345] The fundraising auction effort was ultimately a failure.[346] On April 8, 2017, the Shadow Brokers publicly released the password to this encrypted cache of files.[347]

On April 14, 2017, the group released by far the most damaging leaks to date, including a Microsoft Windows zero-day exploit known as ETERNALBLUE.[348] This exploit—despite the fact Mi-

---

[343] *See* Sanger, *supra* note 337; *see also* Dan Goodin, *Confirmed: Hacking Tool Leak Came from 'Omnipotent' NSA-Tied Group*, ARS TECHNICA (Aug. 16, 2016, 5:09 PM), https://arstechnica.com/security/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/.

[344] *See* Lorenzo Franceschi-Bicchierai, *NSA Targeted Chinese Firewall Maker Huawei, Leaked Documents Suggest*, MOTHERBOARD (Aug. 24, 2016, 9:00 AM), https://motherboard.vice.com/en_us/article/nsa-huawei-firewalls-shadow-brokers-leak.

[345] *See* Joseph Cox, *They're Back: The Shadow Brokers Release More Alleged Exploits*, MOTHERBOARD (Apr. 8, 2017, 11:33 AM), https://motherboard.vice.com/en_us/article/theyre-back-the-shadow-brokers-release-more-alleged-exploits.

[346] *See* Janus Kopfstein, *"Shadow Brokers" Whine3 that Nobody Is Buying Their Hacked NSA Files*, MOTHERBOARD (Oct. 1, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files.

[347] *See* Cox, *supra* note 345.

[348] *See* Dan Goodin, *NSA-Leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet*, ARS TECHNICA (Apr. 14, 2017, 1:27 PM), https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

crosoft issued a patch for it in March 2017, leading some commentators to speculate the company had been tipped off about it[349]—was subsequently used in the massive ransomware attack, known as WannaCry, that has infected over a quarter-million machines to date.[350] The WannaCry virus has since been linked to a hacker group affiliated with North Korea, which has been responsible for multiple sophisticated attacks, including the 2014 attack against Sony Pictures.[351]

B. *CIA and Wikileaks*

Yet another installment in the saga of intelligence community data hacks is the WikiLeaks exposure of CIA cyber tools during March 2017.[352] *The New York Times* reported that the documents were "detailed, highly technical catalogue of tools" and "include[d] instructions for compromising a wide range of common computer tools for use in spying: the online calling service Skype; Wi-Fi networks; documents in PDF format; and even commercial antivirus programs . . . used by millions of people . . . ."[353] WikiLeaks' initial release "of secret C.I.A. material, included 7,818 web pages with 943 attachments, many of them partly redacted by Wikileaks editors to avoid disclosing the actual code for cyberweapons. The entire archive of C.I.A. material consists of several hundred million lines of computer code, the group claimed."[354]

VII. TOPICS FOR FUTURE RESEARCH

The following topics for future research seem to be particularly promising: how will the huge amount of data generated from IoT devices be preserved? What legal framework is needed to protect privacy interests?

---

349 Richard Lawler, *Microsoft Says It Already Patched 'Shadow Brokers' NSA Leaks*, ENGADGET (Apr. 15, 2017), https://www.engadget.com/2017/04/15/microsoft-says-it-already-patched-several-shadow-brokers-nsa-l/.

350 *See* Perlroth & Sanger, *supra* note 341.

351 *See id.*

352 *See* Scott Shane, Matthew Rosenberg & Andrew W. Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

353 *Id.*

354 *Id.*

As billions of IoT sensors and devices come to occupy our physical environment, Richard S. Whitt warns:

> Many of these systems would be collecting, analyzing, and storing often critical data across entire sectors of the economy. It may be misguided to expect that sensors placed in the field will continue providing useful data for their expected lives of years, even decades. Many such devices are doomed to become useless "abandonware" after supporting cloud services are altered or discontinued. Even those in continuing operation risk becoming insecure.[355]

Many of the issues raised in this article have wide-ranging implications, including on both criminal procedure and substantive criminal law.[356] How to apply criminal law to malware and digital weapons has recently been in the news. A security researcher named Marcus Hutchins, who helped prevent the spread of the WannaCry ransomware virus in early 2017, was arrested by the FBI on August 2, 2017.[357] The indictment charges Hutchins with "creating and distributing the Kronos banking trojan," which is a piece of malware that harvests online banking credentials and credit card data.[358] The indictment discusses that an as-yet arrested unnamed coconspirator facilitated selling the malware that Hutchins allegedly created.[359] As

---

355 Richard S. Whitt, "*Through a Glass, Darkly" Technical, Policy, and Financial Actions to Avert the Coming Digital Dark Ages*, 33 SANTA CLARA HIGH TECH. L.J. 117, 134 (2017) (footnotes omitted).

356 *See, e.g.*, Ormerod & Trautman, *supra* note 19 (manuscript at 15).

357 *See* Joseph Cox, *Researcher Who Stopped WannaCry Ransomware Detained in US After Def Con*, MOTHERBOARD (Aug. 3, 2017, 12:22 PM), https://motherboard.vice.com/en_us/article/ywp8k5/researcher-who-stopped-wannacry-ransomware-detained-in-us-after-def-con.

358 Joseph Cox, *WannaCry Researcher Indicted for Allegedly Creating Banking Malware*, MOTHERBOARD (Aug. 3, 2017, 3:07 PM), https://motherboard.vice.com/en_us/article/pagn7v/malwaretech-wannacry-indictment-kronos-malware.

359 *See id.*

Professor Orin Kerr has discussed, the case presents a difficult issue of criminal law: whether it is a crime to create and sell malware.[360]

Of our hyper-connected future world, Samuel Greengard warned, "[a]lready, serious concerns exist about whether this technology will dumb down society, lead to greater inequality, and expand the digital divide."[361] Greengard raised further questions:

> Could automation cause massive unemployment and downward mobility[?] Could it cause more crime or new types of terrorism and warfare? How might it change the legal system? What about the growing problem with digital distraction? . . . How do we approach security and privacy in an era where almost no movement or activity goes unnoticed or unrecorded?[362]

VIII. CONCLUSION

The Stuxnet virus represents a paradigm-shifting event. Stuxnet reveals to the world that a traditional military is no longer necessary to wreak havoc on other countries' military and civilian infrastructure installations. The implications for this shift are wide ranging and innumerable.

Yet, the current climate within critical infrastructure industry fails to grapple with the ramifications of Stuxnet. Both industry and governments are unprepared to respond to a malware infection that renders worthless the systems that developed countries rely on for necessities as basic as food, water, telecommunications, and electricity.

---

[360] *See* Orin Kerr, Opinion, *The Kronos Indictment: Is It a Crime to Create and Sell Malware?*, WASH. POST (Aug. 3, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/03/the-kronos-indictment-it-a-crime-to-create-and-sell-malware/?utm_term=.e3b71b7bfda2.

[361] *See* Greengard, *supra* note 74, at xvii.

[362] *Id.*