RATS, TRAPS, AND TRADE SECRETS

ELIZABETH A. ROWE*

Abstract: Technology has facilitated both the amount of trade secrets that are now stored electronically, and the rise of cyber intrusions. Together, this has created a storm perfectly ripe for economic espionage. Cases involving unknown or anonymous offenders who may not be in the United States and who steal trade secrets using remote access tools ("RATs") are especially problematic. This Article is the first to address and place trade secret misappropriation within the larger backdrop of cybersecurity. First, it argues that systemic issues related to technology will continue to make legislative and judicial solutions suboptimal for cyber misappropriation. Second, it explores how the rhetoric of war has infiltrated the national discourse on cybersecurity and cyber misappropriation. Third, the Article introduces and coins the acronym TRAP. Standing for "technologically responsive active protection," TRAP serves as a guiding principle to further refine the reasonable efforts requirement for the protection of trade secrets. The Article also critically examines such active defense counterstrike techniques as hacking back and the controversy surrounding this potential strategy.

INTRODUCTION

Trade secrets are arguably more important to companies now than ever before in our history. In fact, since the most recent revisions to our patent laws, many believe that trade secrets might be even more important than patents.[1] Accordingly, the theft of trade secrets or trade secret misappropriation from company employees and from outsiders, such as competitors and foreign governments, is on the rise. Facilitating that ascent is technology. We live in a world where the most sensitive proprietary information can be carried on a

* Feldman Gale Professor in Intellectual Property and Director, Program in Intellectual Property Law, University of Florida Levin College of Law. I appreciate comments received from participants at the 2014 Trade Secrets and Information Policy Workshop at the University of Florida, as well as various discussions with Lyrissa Lidsky, Andrea Matwyshyn, and Sharon Sandeen. Thank you also to Nicholas Camillo, Corvis Richardson, Kristen Weigel-Van Aken, and Eric Van Wiltenburg for outstanding research assistance, and to the University of Florida Levin College of Law for its research support.

[1] *See, e.g.*, David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104–06 (2012); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 330 (2008); Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 943 (2012).

mobile device in one's pocket or stored without a device "in the cloud."[2] Although technology has made it easy to store vast amounts of data constituting trade secret information electronically, the Internet and the rise of cyber intrusions into computer systems and networks have created a storm perfectly ripe for corporate espionage and trade secret misappropriation.[3] This Article refers to that type of activity as cyber misappropriation.

Corporate espionage, particularly from foreign countries, is a significant problem for U.S. companies, with some even characterizing it as a war. But the true extent of the problem is unclear. Although some believe it is on the scale of warfare, others are more skeptical.[4] Because the figures are difficult to verify, they might be exaggerated.[5] The rhetoric may also be hyperbolic. Nevertheless, we know that corporate espionage and the theft of trade secrets from American companies is a problem and will continue to be one. The list of companies that have been affected by trade secret misappropriation, either internally from employees or externally from hackers, is striking.[6] Given the intangible nature in which trade secrets exist today, it comes as no surprise that these digital threats are so pervasive.[7]

What makes the problem so urgent, elusive, and significant is that we do not appear to have any effective judicial or legislative tools with which to address it.[8] Rather, it presents peculiar challenges for which our existing legal

---

[2] *See generally* Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. 1 (2014) (examining the impact of cloud storage services on trade secrets and their protection).

[3] *See* ERIC M. DOBRUSIN & RONALD A. KRASNOW, INTELLECTUAL PROPERTY CULTURE: STRATEGIES TO FOSTER SUCCESSFUL PATENT AND TRADE SECRET PRACTICES IN EVERYDAY BUSINESS 264–67 (2d ed. 2012); Aaron J. Burstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionag*e, 41 ARIZ. ST. L.J. 933, 944–46 (2009).

[4] *See infra* notes 92–198 and accompanying text (Part III, examining the rhetoric of war that is now being applied to the issue of cybersecurity); *e.g.*, S. Kumar, *Here's Why You Shouldn't Take US-China Hacking Tensions Too Seriously*, FORTUNE (June 8, 2015, 8:36 AM), https://fortune.com/2015/06/08/heres-why-you-shouldnt-take-us-china-hacking-tensions-too-seriously/ [https://perma.cc/G796-QFGM] (explaining why the threat of a cyberwar between the United States and China is largely overblown and unlikely to happen).

[5] *See, e.g.*, Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172, 196–200 (2014).

[6] For example, the author has compiled a list of victim companies for which trade secret thefts have been prosecuted under the Economic Espionage Act between 2008 and 2013. Among those companies represented are: Goodyear, Korn/Ferry International, Motorola, Boeing International, CISCO, NASA, SiRF Technology, Goldman Sachs, Societe Generale, GM Motor Company, E.I. du Pont de Nemours, Ford Motor Company, Valspar Corporation, Akamai Technologies, Inc., Frontier Scientific, Inc., Cargill, Dow Chemical Company, Sanofi-Aventis, CME Group, L-3 Communications, Teijin Limited, Orbit Irrigation Products, Pittsburgh Corning Corporation, and AMSC.

[7] *See* Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 14–26 (2009).

[8] *See* Elizabeth A. Rowe & Daniel M. Mahfood, *Trade Secrets, Trade, and Extraterritoriality*, 66 ALA. L. REV. 63, 64–66 (2014).

and regulatory framework is not well suited. Although trade secret misappropriation occurring within the United States and involving known offenders, such as employees, can be redressed in civil litigation, the same is not true for cyber misappropriation that originates abroad.[9] Of particular concern, and the focus of this Article, are the types of cases that involve unknown or anonymous offenders, who may or may not be in the United States, and who steal trade secrets through hacking or other breaches of cybersecurity that involve remote access tools ("RATs"). A RAT can remotely control a victim's computer and access their files.[10] Accessing targets remotely without needing to be on the same premises has opened up the world of potential perpetrators and sets up an unwieldy cat and mouse game.

The challenges in this area demonstrate how advances in technology have far outpaced the law. Indeed, it may always be that the law will never be sufficiently nimble to adapt to and keep pace with the cyber world. Effectively addressing cyber misappropriation requires a holistic approach that must involve self-help on the part of trade secret holders. Reliance on the government, law enforcement, criminal laws, and other legal and judicial remedies have not been successful, and it is unlikely that, standing alone, they ever will be.

The Article begins in Part I by briefly framing the foreign economic espionage problem.[11] Part II reviews the current legislative remedies available under both the Economic Espionage Act and the Computer Fraud and Abuse Act for addressing cyber misappropriation, and explains why the technological landscape makes them ineffective.[12] Part III then discusses the war rhetoric that often surrounds cyberattacks and the forces that threaten to make this narrative counterproductive.[13] In Part IV, the Article critically explores an approach focused more on self-help and self-defense, integrating both technological and human considerations.[14] It also considers supplementary initiatives that may further contribute to a more comprehensive approach to the problem of cyber misappropriation, such as a focus on small companies, and government initiatives both in the United States and abroad.[15] Finally, the Article concludes that companies must look inward and re-conceptualize their roles, not as bystanders or onlookers, but as participants responsible for building their own technologically responsive active protection ("TRAPs") and fortresses to protect their trade secrets and proprietary information.

---

[9] *See id*. at 69–72.

[10] *See* United States v. Yücel, 97 F. Supp. 3d 413, 416 (S.D.N.Y. 2015) (providing a description of a RAT and how it is used).

[11] *See infra* notes 16–35 and accompanying text.

[12] *See infra* notes 36–91 and accompanying text.

[13] *See infra* notes 92–198 and accompanying text.

[14] *See infra* notes 199–298 and accompanying text.

[15] *See infra* notes 299–328 and accompanying text.

I. THE THREAT OF FOREIGN ECONOMIC ESPIONAGE

The reports, surveys, and stories are plentiful and paint a vivid picture. A cyber espionage unit of the Chinese army breached 115 American companies over the course of several years.[16] Companies are being attacked at least once a week.[17] Cyber criminals have stolen up to $1 trillion worth of intellectual property in a single year.[18] It is no wonder then that cybersecurity is treated as a national security matter, not just one related to criminal or intellectual property law.[19] Indeed, the narrative and rhetoric in the media, as well as among politicians, tends to make national security the focus of the problem.[20] The government has also taken note and focused attention on the problem.[21] Although that attention is a welcome and necessary component to combating these challenges, the question arises as to what role the private sector ought to play in the process, and whether the importance of that role is diminished by the national security focus.

International espionage of American trade secrets continues to receive increasing attention.[22] In early February 2013, a government report detailed the "unrelenting campaign of cyberstealing linked to the Chinese government."[23] The report identified a group of hackers run by the Chinese People's Liberation Army, Unit 61398,[24] and described a "sophisticated, systematic effort that is allegedly condoned, supported, and directed by the Chinese government."[25] Shortly thereafter, President Obama announced new efforts to prevent the theft of U.S. trade secrets abroad.[26] The White House coordinator of intellectual

---

[16] *See* MANDIANT CONSULTING, APT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 21 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [https://perma.cc/KA63-CLHS].

[17] *See* PONEMON INST., SECOND ANNUAL COST OF CYBER CRIME STUDY: BENCHMARK STUDY OF U.S. COMPANIES 2 (2011), http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf [https://perma.cc/3LQ3-WJJW].

[18] *See* Press Release, The White House, Office of the Press Sec'y, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [https://perma.cc/233J-BNGP].

[19] *See infra* notes 130–154 and accompanying text.

[20] *See infra* notes 22–29 and accompanying text.

[21] *See infra* notes 22–29 and accompanying text.*id.*

[22] *See, e.g.*, Almeling, *supra* note 1, at 1109–12; *see also* Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 241–42 (2010) ("Although threats of economic and industrial espionage have long existed, the international proliferation of the Internet makes cyber economic and industrial espionage an especially daunting and potentially economy-crippling threat."); Rowe & Mahfood, *supra* note 8, at 68.

[23] *See* Lolita C. Baldor, *US Ready to Strike Back on China Cyberattacks*, YAHOO! NEWS (Feb. 19, 2013, 5:43 PM), http://news.yahoo.com/us-ready-strike-back-china-cyberattacks-224303045--finance.html [https://perma.cc/6N8A-RABF].

[24] *See id*.

[25] Rowe & Mahfood, *supra* note 8, at 68.

[26] *See* EXEC. OFFICE OF THE PRESIDENT OF THE U.S., ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 1–12 (2013), http://www.whitehouse.gov/sites/default/files/

property enforcement laid out the "whole of government" efforts that would be utilized to combat international theft of U.S. trade secrets.[27] The White House strategy consisted of five components:

> First, we will increase our diplomatic engagement [and] convey our concerns to countries where there are high incidents of trade secret theft . . . . Second, we will support industry-led efforts to develop best practices to protect trade secrets . . . . Third, [the Department of Justice] will continue to make the investigation and prosecution of trade secret theft by foreign competitors and foreign governments a top priority. . . . Fourth, . . . we will conduct a review of our laws to determine if further changes are needed to enhance enforcement. . . . Lastly, we will increase public awareness of the threats and risks to the U.S. economy posed by trade secret theft.[28]

The precise numbers and actual extent of economic espionage is difficult to ascertain.[29] General Keith Alexander, former Director of the National Security Agency and Chair of the U.S. Cyber Command, has indicated that the amount of intellectual property theft in the United States through cyber espionage is "astounding."[30] Estimates are that we lose hundreds of billions of dollars annually, both from the public and private sector, as a result of this kind of activity.[31] For a whole host of reasons, however, an accurate number is difficult

---

omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [https://perma.cc/FB9Z-VDAS].

[27] Victoria Espinel, *Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets*, WHITE HOUSE BLOG (Feb. 20, 2013, 2:59 PM), https://www.whitehouse.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets [https://perma.cc/YRH8-K8DT]; *see* Ellen Nakashima, *U.S. Launches Effort to Stem Trade-Secret Theft*, WASH. POST (Feb. 20, 2013), http://articles.washingtonpost.com/2013-02-20/world/37198630_1_trade-secret-theft-trade-secrets-commercial-secrets [https://perma.cc/77M6-ETGC] (discussing the Obama Administration's new efforts to combat the theft of U.S. trade secrets).

[28] Espinel, *supra* note 27; *see* Ellen Nakashima, *U.S. Said to Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html [https://perma.cc/N8FV-SM3W] ("The problem with foreign cyber-espionage is not that it is an existential threat, but that it is invisible, and invisibility promotes inaction.").

[29] *See* Rowe & Mahfood, *supra* note 8, at 68.

[30] *See* Keith Alexander, Remarks on Cyber Security Threats to the U.S. (July 9, 2012) http://www.c-span.org/video/?306956-1/cybersecurity-threats-us (commenting on the rate of intellectual property theft at minute 42:36).

[31] *See, e.g.*, Noah C.N. Hampson, *Hacktivism: A New Breed of Protest in a Networked World*, 35 B.C. INT'L & COMP. L. REV. 511, 516 (2012) ("Hackers are responsible for identity theft, fraud, commercial espionage, and other crimes with an annual cost in the trillions of dollars."); J.P. London, *Made in China*, PROC. MAG., Apr. 2011, at 54, *available at* http://www.usni.org/magazines/proceedings/2011-04/made-china #footnotes [https://perma.cc/G3CP-JCP9] ("Cyber espionage alone is estimated to cost the United States up to $200 billion a year.").

to calculate. For one thing, companies often are not aware that they have been victimized.[32] Even when discovered, there is no reliable method for determining and estimating actual losses. Rather, it is left to each individual company to disclose the amount of its loss, if it chooses to acknowledge or publicly disclose at all.

It is unlikely that new legislation will adequately address the breadth of problems presented by economic espionage and cyber misappropriation.[33] Recent attempts at trade legislation have yielded only partial and limited fixes.[34] The reality is that risks are everywhere, whether they are malware-based attacks, intrusions on networks, potential attacks on mobile devices, or potential cloud-based attacks.[35] Thoughtful consideration of this complex issue requires recognition of its place within the larger context of cybersecurity, where all kinds of information, from personal consumer information to military secrets, can be targeted. In that vein, cyber misappropriation—defined here as the theft of trade secrets resulting from cyberattacks—is intertwined with the national discourse on and rhetoric that accompanies cyberattacks, as well as the shortcomings of existing laws that govern trade secret misappropriation.

---

[32] *See infra* notes 85–88 and accompanying text (Part II.C.2).

[33] *See generally* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015) (critiquing and providing arguments against addressing the issue of trade secrecy through federal legislation).

[34] *See* Rowe & Mahfood, *supra* note 8, at 69 (discussing ineffective attempts at legislative fixes). For example,

> [T]he Theft of Trade Secrets Clarification Act of 2012 . . . amended the Economic Espionage Act of 1996 (EEA) by expanding the scope of prohibited conduct and increasing the maximum penalties. The amendment closes the loophole identified in *United States v. Aleynikov* . . . by redefining a trade secret to include processes used internally in connection with services used in commerce. In addition, the Foreign and Economic Espionage Penalty Enhancement Act of 2012 increased penalties for violations of the EEA, but only for those in § 1831, which targets only trade secret theft intended to benefit a foreign government, agent, or instrumentality. Foreign and Economic Espionage Penalty Enhancement Act, Pub. L. No. 112-269, 126 Stat. 2442 (2013); 18 U.S.C. § 1831. These amendments, while potentially helpful in a handful of specific contexts, offer only a piecemeal approach to addressing a problem that would be more effectively and comprehensively addressed by increasing the usefulness of laws that already exist. In this way, and by creating a perception that the problem has been solved, relatively modest legislative modifications have the potential to do more harm than good.

Id. at 69 n.35 (citations omitted).

[35] *See generally* SYMANTEC, INTERNET SECURITY THREAT REPORT 20, at 6 (2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf [https://perma.cc/W8KD-22VM] ("identify[ing], analyz[ing], and provid[ing] informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam").

II. CURRENT LEGISLATIVE WEAPONS

The two main pieces of legislation that can be used to address the misappropriation of trade secrets through cyber misappropriation at a national level are the Economic Espionage Act ("EEA")[36] and the Computer Fraud and Abuse Act ("CFAA").[37] Along with the CFAA, there are a number of other federal laws that address or touch on cybersecurity, including several regulations within the jurisdiction of the Federal Trade Commission.[38] For the purposes of this Article, however, these other federal laws and regulations are not directly applicable.

A. The Economic Espionage Act

To date, the EEA is the only federal law on trade secret misappropriation in the United States. It is a criminal statute. Although there have been repeated calls for a federal civil law on trade secret misappropriation, there is currently no civil counterpart to the EEA. Additionally, unlike the Computer Fraud and Abuse Act, discussed in section B below,[39] the EEA does not currently create a private right of action.[40]

Generally, the EEA gives federal authorities, under the auspices of the U.S. Department of Justice and local federal prosecutors, the power to investigate and prosecute individuals or companies who engage in criminal trade secret misappropriation.[41] Judging from the indictments that have been brought under the EEA, the vast majority of prosecutions involve employees, former employees, and other company "insiders."[42] Acts of corporate espionage by outsiders, however, are also covered by the EEA.[43]

The prototypical EEA case involves employees who violate their duty of confidentiality or loyalty by using or disclosing their employer's confidential business information. For example, in July 2010, two individuals were indicted for stealing and selling $40 million worth of trade secret information related to General Motors' hybrid automobile plans.[44] The allegations were that the employees downloaded and saved confidential General Motors' documents and

---

[36] 18 U.S.C. §§ 1831–1839 (2012).

[37] 18 U.S.C. § 1030 (2012).

[38] *See* Janine S. Hiller & Roberta S. Russell, *The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison*, 29 COMPUTER L. & SECURITY REV. 236, 239 (2013).

[39] *See infra* notes 61–70 and accompanying text (Part II.B).

[40] Legislation has been proposed and is currently pending. *See* Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Trade Secrets Protection Act of 2014, H.R. 5233, 113th Cong. (2014).

[41] *See* 18 U.S.C. §§ 1831–1839.

[42] The author collected and analyzed a selection of indictments that have been brought under the EEA.

[43] *See* 18 U.S.C. § 1832(a).

[44] Indictment at 4, United States v. Qin, No. 10-cr-20454-MOB-RSW (E.D. Mich. July 22, 2010).

then gave the information to a Chinese automaker. This is representative of a large number of EEA prosecutions in which Chinese nationals are over-represented relative to other countries.[45]

Sections 1831 and 1832 of the EEA define the prohibited conduct under the Act.[46] Moreover, the decision of which of the two sections to apply turns on whether the theft was intended to benefit a foreign government. If so, the conduct falls under § 1831.[47] Section 1832, in contrast, governs all other thefts of trade secrets.[48] It applies when there is "intent to convert a trade secret . . . related to a product or service used in or intended for use in interstate or foreign commerce."[49] The accused must intend or know that the conversion will harm the trade secret owner.[50] Both § 1831 and § 1832 make an attempt to steal and a conspiracy to steal trade secrets a crime.[51] Thus, it is conceivable that someone may be prosecuted under the EEA even though no trade secrets were, in fact, stolen. As one court has explained: "[T]o find a defendant guilty of conspiracy, the prosecution must prove (1) that an agreement existed, (2) that it had an unlawful purpose, and (3) that the defendant was a voluntary participant."[52]

Section 1839 of the EEA defines trade secrets broadly.[53] A "trade secret" is information that "the owner thereof has taken reasonable measures to keep . . . secret," and that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."[54] In order to establish a violation of the EEA, federal government prosecutors must prove: "(1) that the information is actually secret because it is neither known to, nor readily ascertainable by, the public; (2) that the owner took reasonable measures to maintain that secrecy; and (3) that independent economic value was derived from that secrecy."[55] The language of § 1839(3) further provides that information is to be protected regardless of its form.[56] Thus, information in electronic or intangible form is pro-

---

[45] Based on the author's examination of EEA indictments from 2008 to 2013, thirty-two of fifty defendants were Chinese nationals. The countries with the next highest numbers were South Korea (eight) and the United States (five). The sources consulted for this analysis are on file with the author.

[46] 18 U.S.C. §§ 1831–1832.

[47] *See id.* § 1831.

[48] *See id.* § 1832.

[49] *Id.* § 1832(a).

[50] *See id.* (including as an element, "intending or knowing that the offense will . . . injure any owner").

[51] *See id.* §§ 1831(a), 1832(a).

[52] United States v. Martin, 228 F.3d 1, 10–11 (1st Cir. 2000).

[53] *See* 18 U.S.C. § 1839.

[54] *Id.* § 1839(3)(A)–(B).

[55] United States v. Chung, 659 F.3d 815, 824–25 (9th Cir. 2011).

[56] *See* 18 U.S.C. § 1839(3) ("[T]he term 'trade secret' means all forms and types . . . whether tangible or intangible, and whether or how stored . . . .").

tected under the EEA. It is significant that the drafters of the Act (in the early 1990s) had the foresight to include this coverage, given that virtually all trade secret misappropriation today, especially cyber misappropriation, involves trade secrets stored electronically.

In order to address the concern that foreign governments and foreign entities are attempting to steal U.S. trade secrets, the reach of the EEA extends outside the boundaries of the United States. If the theft of a trade secret occurs in a foreign country, jurisdiction may be asserted if: (a) the defendant is a U.S. citizen or corporation, or (b) any "act in furtherance of the offense" was perpetrated within the United States.[57] Unfortunately, this provision has not proven sufficiently useful to be widely utilized. Part of the reason is because prosecutors do not have the appropriate enforcement and service mechanisms to use against individuals who are outside of the United States.

The number of prosecutions under the EEA has been relatively low. Since the Act was passed in 1996, there have been about 100 indictments and few convictions.[58] One reason for this paucity is the fact that prosecutors are unlikely to use their limited resources to prosecute an economic crime where the victim-company has a readily available, and perhaps better suited, civil cause of action and remedy. Many companies also choose not to report espionage to the government for prosecution, with one report noting that in 2005, only about fifteen percent of detected incidents were reported to law enforcement.[59]

Commentators have speculated as to why that may be the case.[60] There are several reasons why a trade secret owner may be disinclined to report a trade secret misappropriation claim to criminal authorities. First, if a report is filed and a criminal prosecution is brought, the trade secret owner effectively loses control of the situation and any parallel civil case may be stayed pending resolution of the criminal case. Second, because the trade secret owner lacks control of criminal proceedings, there is a greater risk that its trade secrets will be exposed (and thereby lost) during the criminal proceeding. Third, there is often a public relations concern if news of trade secret misappropriation becomes public, particularly for publicly-traded companies whose stock prices may be negatively affected.

---

[57] *See id.* § 1837.

[58] *See* COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 42 (2013), http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf [https://perma.cc/WL5S-CAB6].

[59] *See* RAMONA R. RANTALA, BUREAU OF JUSTICE STATISTICS, CYBERCRIME AGAINST BUSINESSES, 2005, at 2 (2008), http://www.justiceacademy.org/iShare/Library-BJS/CyberCrimes.pdf [https://perma.cc/UQX6-MPLV].

[60] *See, e.g.*, Argento, *supra* note 5, at 215–18.

B. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act is a federal law that was adopted (before the advent of the commercial use of the Internet) to address the problem of computer hacking, and it does not directly address trade secret misappropriation.[61] Unlike the EEA, however, it includes a private right of action that some plaintiffs use to bring state trade secret claims before the federal courts. The CFAA makes it a crime for anyone to intentionally access a computer without authorization, or surpass authorization, in order to access "information from any protected computer."[62] Because the principal wrongdoing as defined by the CFAA is "accessing a protected computer," its provisions conceptually overlap with the improper acquisition provisions of trade secret law.[63] Thus, if the facts of a trade secret case involve the acquisition of trade secrets that are stored on a computer, the plaintiff in a civil trade secret case might also pursue a criminal prosecution under the CFAA.

Whether the defendant's access to the subject computer was unauthorized or exceeded existing authorization is at the heart of a CFAA claim. Of particular concern is whether a violation of ubiquitous "terms of use agreements" can make some activities "unauthorized" for purposes of the CFAA.[64] Similar concerns are raised with respect to common provisions of employment agreements and confidentiality agreements that limit computer access.

Sometimes the CFAA, in effect, serves as a federal trade secret law. It can be used to capture those who intentionally access a protected computer without authorization, regardless of whether or not the information accessed was a trade secret.[65] Some courts have interpreted the statute broadly to create liability where employees access data in violation of a general duty of loyalty or confidentiality to the employer. Thus, although the employee may have had access to the computers, violating an employment policy or exceeding authorization to access certain information can create liability.[66] Other courts interpret the statute more narrowly, requiring unauthorized access to the computers ra-

---

[61] *See* 18 U.S.C. § 1030.

[62] *Id.* § 1030(2)(C).

[63] *See generally* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429 (examining the intersection of the CFAA and trade secret misappropriation and resulting harms).

[64] *See* 18 U.S.C. § 1030.

[65] *See generally* Enargy Power Co. v. Xiaolong Wang, No. 13-11348-DJC, 2013 U.S. Dist. LEXIS 170193 (D. Mass. Dec. 3, 2013) (finding that plaintiffs are likely to succeed on their CFAA claim even without a likelihood of success on their trade secret misappropriation claim).

[66] *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (accessing information for a nonbusiness reason is a violation); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that a CFAA violation exists where employee breached his duty of loyalty by destroying files that were his employer's property); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45–46 (D. Mass. 2009) (finding that an employee violated the CFAA by using information in breach of a duty of loyalty to his employer).

ther than merely unauthorized use of information.[67] The broader interpretation creates liability not just for hacking, but for any unauthorized appropriation or use of the data.

It is also worth noting in the context of this Article that the broad framework provided under the CFAA for addressing cyberattacks may also threaten the legitimate work of security researchers. That is because some of the activities and processes that are necessary to identify and assess weaknesses in cybersecurity arguably violate the CFAA.[68] Researchers have complained that when they identify vulnerabilities or bugs in systems and disclose their findings to manufacturers, technology providers, or those otherwise responsible for repairing such weaknesses, they have been threatened with legal action both civilly and criminally.[69] As a result, there have been calls to clarify the CFAA or to explicitly exempt these kinds of research activities from its reach.[70]

C. Why Law Is Not the Answer

The EEA cases almost all involve employees who obtained their employer's trade secrets and transferred them to a competitor, often a foreign competitor. For example, a product development manager downloaded dozens of files containing confidential product information and transferred them to a competitor.[71] A design engineer transported stolen "data sheets" containing his employer's proprietary information to a potential foreign competitor.[72] An employee stole his employer's back-up tapes and offered them for sale to a com-

---

[67] *See* United States v. Nosal, 676 F.3d 854, 859, 863 (9th Cir. 2012) (en banc) ("[W]e hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.").

[68] *See Cyber Crime: Modernizing Our Legal Framework for the Information Age: Hearing Before the S. Judiciary Subcomm. on Crime & Terrorism*, 114th Cong. 1–3 (2015) (statement of Jen Ellis, Senior Dir. of Cmty. & Public Affairs, Rapid7) (discussing how security research is being threatened by current and future legislation, including the CFAA).

[69] *Id.* at 2.

[70] *See, e.g.*, Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537, 541 (2009) (suggesting, for example, an amendment to the CFAA to provide a "safe harbor for ethical hacking").

[71] Press Release, U.S. Dep't of Justice, Former Silicon Valley Engineer Will See Prison After Conviction for Stealing Marvell Trade Secrets (Feb. 25, 2013), http://www.justice.gov/usao-ndca/pr/former-silicon-valley-engineer-will-see-prison-after-conviction-stealing-marvell-trade [https://perma.cc/4SM2-KWP4].

[72] *See* Press Release, U.S. Dep't of Justice, Chip Design Engineer Pleads Guilty to Transporting Stolen Property of Silicon Valley Company to Taiwan (Sept. 6, 2005), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2005/tsaiPlea.htm [https://perma.cc/5RAN-YKC3].

petitor.[73] Finally, an information technology specialist sold his employer's confidential information for $3 million dollars.[74]

Sometimes it is not employees who steal trade secrets, but third parties or others with access to information. In one case, a college student stole sensitive trade secrets belonging to DirecTV while he was working for a copying service employed by DirecTV's outside counsel.[75] In another case, two Harvard Medical School post-doctoral research fellows were accused of stealing marketable scientific information belonging to Harvard.[76] The pair shipped more than thirty boxes of biologicals, books, and documents to a competing lab.[77] They then further collaborated with a Japanese company in the creation and sale of related and derivative products, and otherwise capitalized on the information.[78]

A deeper analysis of the scenarios presented in the facts of these cases reveals some underlying, systemic issues related to technology that will continue to make legislative and judicial solutions suboptimal for cyber misappropriation. Subsection 1 explores how the nature of trade secret information as intangible makes security a challenge.[79] Subsection 2 discusses how the nature of the information through the architecture of the Internet makes it difficult to identify offenders.[80] Finally, subsection 3 examines how, because the Internet has increased the likelihood of offenders being outside of the country, prosecution can be even further hindered.[81]

1. Intangible Information

Trade secret law is the primary area of intellectual property law that covers how we control, protect, acquire, and use information. But this kind of "property" right in information presents a huge challenge because of its present-day form as electronically stored data. The intangible nature of information has significant implications for how we regulate and control that in-

---

[73] Press Release, U.S. Dep't of Justice, Former IT Director of Silicon Valley Company Pleads Guilty to Theft of Trade Secrets (Aug. 1, 2005), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2005/woodwardPlea.htm [https://perma.cc/U7WL-JRLH].

[74] Press Release, U.S. Dep't of Justice, Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information (Apr. 11, 2003), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/sunPlea.htm [https://perma.cc/8ZKC-2QHT].

[75] Press Release, U.S. Dep't of Justice, L.A. Man Sentenced for Stealing Trade Secrets Pertaining to 'Smart Card' Technology (Sept. 8, 2003), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/serebryanySent.htm [https://perma.cc/9YRW-3X6H].

[76] Press Release, U.S. Dep't of Justice, Pair Charged with Theft of Trade Secrets from Harvard Medical School (June 19, 2002), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/zhuCharges.htm [https://perma.cc/4F4W-4WR6].

[77] *Id.*

[78] *Id.*

[79] *See infra* notes 82–84 and accompanying text.

[80] *See infra* notes 85–88 and accompanying text.

[81] *See infra* notes 89–91 and accompanying text.

formation and others' use of it. Indeed, in some ways it is akin to trying to capture air. With real property we can build fences, use locks, and attach alarms. Traditionally, that was the model that we used and developed to protect trade secrets.[82] A new day has come, however, and that model may not serve as well going forward.

The prevalence of cyber misappropriation makes evident the fact that how we capture, corral, and lock up proprietary information has left us wanting and needing more effective mechanisms and tools, from both a legal and business perspective, to better protect our information. In this digital age, securing information can be especially daunting because once a trade secret has been disclosed, even inadvertently, it ceases to be considered as such and loses all protection (unlike a patent).[83] This makes trade secrets extremely vulnerable, and makes misappropriation easier and more prevalent than ever before.[84]

2. Identifying Culprits

The intangible nature of information, when taken from its owner, makes detection of the loss and identification of the culprits particularly difficult.[85] When a trade secret stored in electronic form is stolen, the misappropriator has often taken a copy of the data but left the original intact and in place.[86] Accordingly, it may be a while before anyone notices that the information has been taken, and weeks, months, sometimes even years may pass before the loss is detected.

This delay through the passage of time in and of itself reduces the likelihood that the offender, particularly if he or she was not an employee, might be identified. Granted, if the perpetrator is an employee it can be easier to track and make an identification from the company's computer logs upon discovery of the misappropriation. But when the culprit is on the outside, the situation is more challenging. Compounding the problem is the fact that the architecture of the Internet allows for disguises and makes it difficult to trace the source of an intrusion. Observing certain patterns to identify hackers is not a reliable way to

---

[82] *See* Rowe, *supra* note 7, at 9–10.

[83] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (noting that a person can permanently destroy trade secrets by posting them on the Internet).

[84] *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW 193–95 (2012) (examining the challenges of keeping information protected in today's digital age).

[85] OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011, at 1 (2011) [hereinafter ONCIX REPORT], http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [https://perma.cc/387M-P5NE] (examining some of the factors that make identifying the guilty party so difficult).

[86] *See* United States v. Nosal, 930 F. Supp. 2d 1051, 1054–55 (N.D. Cal. 2013).

identify the source of a hack. Sometimes hackers share tools, which makes it even harder to identify or tie certain tactics to a particular group.[87] It is also possible to hire an independent hacker to infiltrate a system, thus making identification of the true source even more difficult.[88] This can be especially challenging if a hacker is working outside of the country.

3. Cross-Border Incidents

Because it is easier to access intangible information from anywhere in the world, and to do so in a manner that is unlikely to be detected, the Internet has thus vastly expanded the potential threat of actors successfully reaching and accessing American trade secrets. Even when foreign offenders are identified and espionage charges may be filed under the EEA, prosecution in the United States can be severely hindered. Complicating prosecution is the fact that offenders who live outside the United States would need to be extradited back to the United States, and not all countries permit extradition for these types of offenses.[89] Although the EEA includes a provision for extraterritorial jurisdiction for acts of trade secret misappropriation even if outside the United States, in practice it is not a meaningful remedy.[90] Prosecutors do not have the appropriate enforcement and service mechanisms with which to serve individuals and entities that are not located in the United States. In reality, violators cannot fully be charged and indicted under a system unless and until they are within its borders.[91]

III. WHY CYBERWAR IS NOT THE ANSWER

In any discussion of cybersecurity, the rhetoric of war from the government is hard to miss. We are "fighting a cyber-war;"[92] we are at risk for a "cyber-Pearl Harbor."[93] According to the U.S. Department of Defense,

---

[87] *See, e.g.*, MANDIANT CONSULTING, M-TRENDS: THE ADVANCED PERSISTENT THREAT 2 (2010), https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf [https://perma.cc/5ZGV-7GND] (noting inability to determine identities of attackers); *see also* DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 4, 6 (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [https://perma.cc/CG99-RSYV] (same).

[88] *See* ONCIX REPORT, *supra* note 85, at 1.

[89] *See* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 115 (2014).

[90] *See* 18 U.S.C. § 1837 (stating when the statute applies to conduct outside of the United States).

[91] *See* COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., *supra* note 58, at 42.

[92] Mike McConnell, Opinion, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html [https://perma.cc/3B24-T3D5].

[93] Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html [https://perma.cc/H9A4-KQ4S] (quoting former Defense Secretary Leon E. Panetta).

cyberattacks can constitute an "act of war."[94] Words and phrases like attacks, strikes, cyber operations, national security threats, cyber warfare, waging war, geopolitical assaults, and digital battlefield have become commonplace in the narrative about cybersecurity.[95] This Part will evaluate the use and implications of the choice of this rhetoric, and draw parallels to the War on Drugs from the 1980s that might be instructive in placing this current societal challenge against a backdrop of a similarly complex historical issue implicating law and culture.[96]

The rhetoric of war can also be a political marketing tool used to persuade the public to support certain public policy issues.[97] Along with the "War on Drugs" we have had the "War on Poverty," the "Cold War," and the "War on Terror."[98] This metaphorical militaristic rhetoric encourages a focus on a specific enemy that threatens national security (directly or indirectly), potentially frightens or motivates the public to mobilize against the enemy, and engages in a struggle to win no matter how high the financial or other costs (including sometimes those related to civil liberties).[99]

This is not to suggest that the underlying problems targeted by these "wars" are not real or urgent. Nevertheless, it is important to consider the effect that the marketing and presentation of the problem might have not only on the public, but also on policymakers and stakeholders. It is also very important that such rhetoric not stifle or inhibit debate in the exploration of various viewpoints on the issue.[100]

Although the government appears to have recognized and to be taking the threat to and protection of trade secrets very seriously, the rhetoric of war that

---

[94] U.S. DEP'T OF DEF., CYBERSPACE POLICY REPORT 1, 9 (2011), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf [https://perma.cc/H3ZP-2DG2].

[95] *See, e.g.*, Shane McGee et al., *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 3 (2013); Jan E. Messerschmidt, Note, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 292 (2013); Robert Graham, *Obama's War on Hackers*, ERRATA SECURITY BLOG (Jan. 14, 2015), http://blog.erratasec.com/2015/01/obams-war-on-hackers.html#.VXhW82AcJQ2 [https://perma.cc/KM98-NAKL]; Manish Singh, *US Govt Proposes to Classify Cybersecurity or Hacking Tools as Weapons of War*, BETANEWS (May 23, 2015), http://betanews.com/2015/05/23/us-govt-proposes-to-classify-cybersecurity-or-hacking-tools-as-weapons-of-war/#comments [https://perma.cc/J5CJ-AQ88].

[96] *See infra* notes 97–198 and accompanying text.

[97] *See generally* Susan Stuart, *War as Metaphor and the Rule of Law in Crisis: The Lessons We Should Have Learned from the War on Drugs*, 36 S. ILL. U. L.J. 1 (2011) (examining and critiquing the frequent use of a militaristic rhetoric within public policy).

[98] *Id.* at 2–3.

[99] *See id.* at 3–6.

[100] *See* Andrew D. Black, *"The War on People": Reframing "The War on Drugs" by Addressing Racism Within American Drug Policy Through Restorative Justice and Community Collaboration*, 46 U. LOUISVILLE L. REV. 177, 182–84 (2007) (discussing how the harsh metaphor of a war against drugs prevents discussion and quiets opposition).

is beginning to accompany the government's strategy for addressing the problem is likely to be counterproductive and not effective. Moreover, it might lead to a misplaced reliance on the government to address a problem that is, in the first instance, best addressed on a more micro, company level. Not only are putative trade secret owners required to take reasonable efforts to protect their trade secrets, but in the age of cyber intrusions and relatively invisible theft of trade secrets, it is a practical reality that cannot be overlooked. Whatever metaphorical war might be waging between the government and its enemies, there is no substitute for building stronger defenses in the private sector.

A. The Cyberwar

Threats from cyber espionage have been framed as threats to our national security. According to President Obama, it is "one of the most serious economic and national security challenges,"[101] and a "rapidly growing threat."[102] Heads of the FBI and national intelligence agencies have identified the cyber threat as the top global threat facing America,[103] rivaling and even surpassing that of terrorism.[104]

In October 2012, President Obama signed a directive authorizing the federal government to act defensively and counterattack with cyber operations under the Presidential Policy Directive 20.[105] The directive instructs the government to identify potential foreign targets that could be the subject of "Offensive Cyber Effects Operations" if ordered by the President.[106] The directive

---

[101] Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL STREET J. (July 19, 2012), http://www.wsj.com/articles/SB10000872396390444330904577535492693044650 [https://perma.cc/W6SL-5CLZ].

[102] Barack Obama, Remarks by the President in the State of the Union Address (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address [https://perma.cc/8F3T-ACWT].

[103] *See Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 5 (2013) (statement of James R. Clapper, Dir. of Nat'l Intelligence), http://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf [https://perma.cc/2347-M4D4] ("So when it comes to the distinct threat areas, our statement this year leads with cyber. And it's hard to overemphasize its significance.").

[104] *See* Stacy Cowley, *FBI Director: Cybercrime Will Eclipse Terrorism*, CNN MONEY (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm [https://perma.cc/YB23-VQYL] (quoting former FBI Director Robert Mueller as stating: "Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country.").

[105] Memorandum from President Barack Obama to Vice President et al. 9 (Oct. 2012), https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf [https://perma.cc/XC8Y-5ALR] (detailing President Obama's Presidential Policy Directive 20 ("PPD20")). *See generally* Nicholas Ryan Turza, Note, *Counterattacking the Comment Crew: The Constitutionality of Presidential Policy Directive 20 as a Defense to Cyberattacks*, 15 N.C. J.L. & TECH. ONLINE 134 (2014) (discussing PPD20).

[106] *Id.*

appears to recommend preparation of counter cyberattacks against foreign threats, execution of cyber operations in the United States, and implementation of cyber intelligence-gathering against other nations.[107] Although the full extent of what is authorized under this directive remains unclear, as a whole it empowers the National Security Agency to fight cyber espionage by taking both proactive and defensive steps to deter these attacks.[108]

Some commentators have noted the effects of a cyberwar on the criminalization of conduct occurring online. For instance, some point to the aggressive use, expansion, and penalties under the CFAA and question whether it will actually serve as an effective deterrent.[109] Others point to the prosecution of those who download information that was already made public, as well as the move to upgrade hacking to a racketeering offense, which could snare potentially innocent players as members of a "criminal enterprise."[110] In particular, there is concern that cybersecurity professionals and researchers might be at risk due to the potentially overbroad laws or overzealous enforcement.[111]

Concerns have also been raised that the government might effectively be treating hacking as an act of war by equating hacking tools to weapons of war. For instance, a rule proposed by the Bureau of Industry and Security seeks to create a new definition of "intrusion software," making it more difficult to export computer security tools.[112] Security researchers are concerned that these new classifications might inhibit their work.[113]

B. Parallels to the "War on Drugs"

In thinking about the rhetoric of war as used in the context of cyber espionage, and the possible implications stemming from the narrative of war to frame a problem, a useful analogy and point of reference is the earlier "War on Drugs" in the United States. It also serves as a reminder that criminal law, by itself, may not always be the best way to fix behavioral and societal issues, even when those issues appear on a large scale. It is widely believed, even by

---

[107] *See id.* at 4, 6–7.

[108] In the same way, companies would be well served to similarly prepare against attacks and intrusions to their proprietary information.

[109] *See, e.g.*, Hanni Fakhoury, *The U.S. Crackdown on Hackers Is Our New War on Drugs*, WIRED (Jan. 23, 2014, 9:30 AM), http://www.wired.com/2014/01/using-computer-drug-war-decade-dangerous-excessive-punishment-consequences/ [https://perma.cc/8G6Z-8MFA] (questioning the effectiveness of strict prison sentences imposed for CFAA violations).

[110] *See, e.g.*, Graham, *supra* note 95.

[111] *See id.*

[112] *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015) (to be codified at 15 C.F.R. § 772.1).

[113] *See* Singh, *supra* note 95 ("The new proposal is irking security researchers, who find exporting controls on vulnerability research a regulation of the flow of information.").

the current administration, that the war rhetoric was "counterproductive" for drug enforcement.[114]

President George H.W. Bush's first address to the nation in 1989 began, "All of us agree that the gravest domestic threat facing our nation today is drugs."[115] The War on Drugs, which began under the Nixon Administration but intensified under the presidencies of Ronald Reagan and George H.W. Bush, was accompanied by a great expansion of government authority, including wiretapping, search warrants, and civil forfeiture laws.[116] But many have argued that it did not lead to significant positive changes.[117] One lesson for the cyber misappropriation problem might be that more focus is needed on the people and their motivations, rather than a tunnel-vision focus on enforcement. Knowing why people hack, what motivates them to do it, and what they hope to gain from it might actually lead to addressing the problem on a deeper level and place us in a better position to find solutions.[118]

C. Who Is the Enemy?

If news and government reports[119] are any measure, the face of our cyberwar enemy—who must be feared and stopped—is China and its hacking crews. Some refer to it as a "fake war"[120] ongoing between China and the United States, as the two giants hurl accusations and threats against each other for cyber intrusions and theft of trade secrets. Although there is documented evidence that Chinese companies have attempted to steal and have successfully

---

[114] *See* Andrew Glass, *Reagan Declares 'War on Drugs,' October 14, 1982*, POLITICO (Oct. 14, 2010, 4:44 AM), http://www.politico.com/news/stories/1010/43552.html [https://perma.cc/R96F-8SAH].

[115] George H.W. Bush, Address to the Nation on the National Drug Control Strategy (Sept. 5, 1989), http://www.presidency.ucsb.edu/ws/index.php?pid=17472&st=&st1= [https://perma.cc/7A4Y-KML7].

[116] *See* Ross C. Anderson, *We Are All Casualties of Friendly Fire in the War on Drugs*, 13 UTAH B.J. 10, 11–12 (2000). *See generally* Stuart, *supra* note 97 (examining the controversial measures and repercussions of the War on Drugs).

[117] *See, e.g.*, Stuart, *supra* note 97, at 35–41.

[118] *See, e.g.*, Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 394–96 (2014); Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J.L. ECON. & POL'Y 511, 530–31 (2005); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 915–16 (2013).

[119] *See, e.g.*, Thomas Claburn, *China Cyber Espionage Threatens U.S., Report Says*, INFO. WK. DARK READING (Nov. 20, 2009, 2:23 PM), http://www.darkreading.com/risk-management/china-cyber-espionage-threatens-us-report-says/d/d-id/1085047? [https://perma.cc/57HR-ZXGG] (quoting the U.S.-China Economic and Security Review Commission's 2009 report that China's espionage efforts are "the single greatest risk to the security of American technologies").

[120] *See* Kumar, *supra* note 4.

stolen trade secrets from American companies,[121] and indeed there are more prosecutions under the EEA against Chinese citizens than any other group,[122] the precise measure and scale is unknown.[123] Coincidentally, this bears some resemblance to the presence of a common enemy in the War on Drugs.[124] Nevertheless, the fact is that trade secret holders have a universal base of potential enemies from whom to protect their trade secrets. Regardless of the extent of China's involvement in cyber misappropriation, it would be wise not to be distracted by the news media's constant focus on China and its hackers, and focus more on security protocols to protect trade secrets. As one commentator has amusingly noted, "The Chinese are like the Kardashians . . . . [Y]ou mention China in an attack, and every radio or news station picks it up."[125] Thus, taking steps to protect information, no matter who or what the source of the intrusion or misappropriation, must remain the paramount concern. To that end, this section will explore how the Internet, foreign governments, employees, and outside hackers all stand as formidable enemies in the battle to protect companies' crown jewels.[126]

1. The Internet

In previous work I have explained how the Internet is a dangerous place for trade secrets.[127] Those discussions focused on the posting of trade secret

---

[121] Verizon reported that in 2013, about 96% of confirmed breaches involving trade secret espionage came from China. VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 6 n.9, 11 n.21 (2013), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [https://perma.cc/4GJ4-JWVU].

[122] *See supra* note 45 and accompanying text.

[123] For one thing, determining exactly what country a hack came from can be imprecise because, for instance, "someone from China with an IP address associated with them[] may be committing cyber attacks in France." Andrea Huspeni, *Think China Is the No. 1 Country for Hacking? Think Again*, NBC NEWS (Oct. 16, 2013, 2:46 PM), http://www.nbcnews.com/id/53297949/ns/business-small_business/t/think-china-no-country-hacking-think-again/#.VqE4dzY4mt8 [https://perma.cc/YQN2-VP9E].

[124] *Compare* Black, *supra* note 100, at 178 (explaining how blacks were disproportionately affected by the War on Drugs), *with* Andrea Shalal & Jim Finkle, *U.S. May Act to Keep Chinese Hackers out of Def Con Hacker Event*, REUTERS (May 24, 2014, 5:16 PM), http://www.reuters.com/article/2014/05/24/us-cybercrime-usa-china-idUSBREA4N07D20140524 [https://perma.cc/GTB2-LVBU] (reporting that the U.S. government was using visa restrictions to prevent Chinese nationals from attending the 2014 Def Con and Black Hat conferences).

[125] Mathew J. Schwartz, *Don't Blame China for Security Hacks, Blame Yourself*, INFO. WK. DARK READING (Feb. 25, 2013, 10:27 AM), http://www.darkreading.com/vulnerabilities-and-threats/dont-blame-china-for-security-hacks-blame-yourself/d/d-id/1108794? [https://perma.cc/K7N3-SZQA] (quoting former Gartner analyst John Pescatore).

[126] *See infra* notes 127–198 and accompanying text.

[127] *See generally* Rowe, *supra* note 7 (applying principles of contributory negligence to the current legal treatment of trade secrets); Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041 (arguing for takedown legislation to help protect trade secrets on the Internet); Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Se-*

information on the Internet by employees or outsiders, and the resulting loss of trade secret protection from that conduct. This Article views the Internet danger from a different angle: as a borderless medium that allows stealth intrusions (and thus misappropriation) of trade secrets by anyone from anywhere in the world. In addition, the interconnected nature of the Internet provides the tie that binds governments and businesses, public and private sectors, and national and international parties. It provides the ease and the framework with which intruders can infect systems, ultimately affecting individual businesses and large-scale economies in the process.[128]

The tools available for those interested in committing cybercrimes have become widely available, and are not reserved for those with the highest levels of training and expertise. In fact, there is a hot and active market for "zero-day" exploits, Trojans, botnets, and other do-it-yourself kits, as well as easy connections between buyers and sellers in this underworld.[129] This easy access and entry for those with malicious motivations place trade secrets at significant risk.

2. Foreign Governments

Foreign governments have used strategic cyberattacks in growing numbers,[130] and some view these as geopolitical assaults on the United States.[131] Alleged threats from Syria, China, and Russia illustrate how the problem becomes a national security threat rather than simply an economic issue.[132] Even

---

quential Preservation, 42 WAKE FOREST L. REV. 1 (2007) (discussing how trade secrets can be lost when posted online).

[128] *See* Hiller & Russell, *supra* note 38, at 237.

[129] *See, e.g.*, RSA, 2012 CYBERCRIME TRENDS REPORT: THE CURRENT STATE OF CYBERCRIME AND WHAT TO EXPECT IN 2012, at 5 (2012), http://www.cs.toronto.edu/~lloyd/TKF/TKF11/11634_CYBRC12_WP_0112.pdf [https://perma.cc/5N92-EYM5] (describing the underground marketplace for cyber fraud); Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:43 AM), https://web.archive.org/web/20160213112132/http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#818495f217bf (documenting the black market for so-called "zero-day" exploits, a hacking technique benefiting from hidden weaknesses in software, or "cyberweaponry"); Stew Magnuson, *Growing Black Market for Cyber-Attack Tools Scares Senior DoD Official*, NAT'L DEF. MAG. (Feb. 22, 2013, 2:49 PM), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1064 [https://perma.cc/QU7M-SVJC]; Derek Manky, *Why Cybercrime Remains Big Business—And How to Stop It*, FORBES (Feb. 1, 2013, 5:07 PM), https://web.archive.org/web/20151003080820/http://www.forbes.com/sites/ciocentral/2013/02/01/why-cybercrime-remains-big-business-and-how-to-stop-it/.

[130] Perhaps the U.S. government has used these tactics as well. *See* McGee et al., *supra* note 95, at 2–3 (discussing the U.S. government's approach to using offensive cyber capabilities).

[131] *See* Brandon Valeriano & Ryan Maness, *Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare*, *in* CYBERSPACE AND NATIONAL SECURITY 139, 144 (Derek S. Reveron ed., 2012).

[132] *See Cybersecurity: Assessing the Immediate Threat to the United States: Hearing Before the Subcomm. on Nat'l Sec., Homeland Def. & Foreign Operations of the H. Comm. on Oversight &*

countries that one may not necessarily think of as a hacking center, like Indonesia, may nonetheless still serve as a formidable opponent in the hacking war.[133] Commentators have discussed the ways in which these foreign countries have infiltrated and attacked targets in the United States, generally gaining access to the media, the providers of public infrastructure services, and implicating more than trade secrets.[134] There is even a real-time world map that one can view to observe attack origins and targets as they occur.[135]

Many countries, including Russia, France, Israel, India, Japan, Taiwan, and China, allegedly engage in cyber espionage against U.S. companies. In our rhetoric of war, however, one public enemy emerges in the narrative, and that appears to be China.[136] According to one public official, "[The Chinese] are stealing everything that isn't bolted down, and it's getting exponentially worse."[137] One report accuses the Chinese of being "the world's most active and persistent perpetrators of economic espionage."[138] The close relationship between the Chinese military and its state-owned companies might also contribute to its position as chief culprit. The U.S. government believes that up to fifty percent of the Chinese economy is controlled by the state, and that industrial espionage is an articulated mission of its intelligence services.[139] Both the government and private companies have also implicated China in alleged thefts of proprietary and trade secret information.[140]

Gov't Reform, 112th Cong. 26 (2011) (prepared statement by James A. Lewis, Dir., Tech. and Pub. Policy Program, Ctr. for Strategic & Int'l Studies).

[133] *See* Shalal & Finkle, *supra* note 124 (noting that in 2013 the majority of global cyberattacks came from Indonesia).

[134] *See, e.g.*, Turza, *supra* note 105, at 137–45.

[135] Heather Timmons, *Watch the Global Hacking War in Real Time with a Weirdly Hypnotic Map*, QUARTZ (June 23, 2014), http://qz.com/224618/watch-the-global-hacking-war-in-real-time-with-a-weirdly-hypnotic-map/ [https://perma.cc/5Z9T-RUJN] (describing the map, created by a company that monitors spyware and malware, allegedly showing cyberattacks around the world; available at http://map.ipviking.com [https://perma.cc/G3KF-UPYP]).

[136] *See supra* notes 119–125 and accompanying text.

[137] Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG BUS., (Dec. 14, 2011, 8:47 A.M.), http://www.bloomberg.com/news/articles/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war [https://perma.cc/3NBY-WF5M].

[138] *See* COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., *supra* note 58, at 15 (quoting the U.S. National Counterintelligence Executive).

[139] *See* U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2012 REPORT TO CONGRESS 155–56 (2012), http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf [https://perma.cc/V3PR-B4Y2]; Mike McConnell et al., *China's Cyber Thievery Is National Policy—And Must Be Challenged*, WALL STREET J. (Jan. 27, 2012), http://www.wsj.com/articles/SB10001424052970203718504577178832338032176 [https://perma.cc/2RNR-MLKR].

[140] *See, e.g.*, ONCIX REPORT, *supra* note 85, at 5; BRYAN KREKEL ET AL., NORTHROP GRUMMAN, OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE 6–13 (2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf [https://perma.cc/VG7Z-L345]; David Barboza, *In Wake of Cyberattacks, China Seeks New Rules*, N.Y. TIMES (Mar. 10, 2013), http://www.nytimes.com/2013/

China has denied the allegations and has stated its official position against hacking.[141] Chinese Premier Li Keqiang also seeks an end to the "groundless accusations,"[142] and Chinese diplomats have denounced reports of Chinese espionage as "baseless, unwarranted and irresponsible."[143] Moreover, because hackers can disguise the source of their attacks by spoofing an Internet Provider address ("IP address"), it is possible that attacks that appear to be coming from China might actually have originated elsewhere, including within the United States.[144] Whether the enemy is a Chinese attacker, a Russian crime group, or an angry former employee, a focus on protecting and defending one's own proprietary information, rather than relying on the government to fight an enemy or battle, is ultimately the most productive and effective way to stem the loss of company trade secrets.

In a recent case, a group of Chinese defendants were indicted under the EEA and the CFAA for wide-scale theft of trade secrets against several American companies, spanning from 2006 to 2014.[145] This case provides an illustration of the ways in which foreign governments or entities can use technology to obtain access to and steal trade secrets. According to the indictment, members of the Chinese military conspired to hack into the computer systems of several businesses in order to steal trade secret information for the benefit of Chinese competitors.[146] For instance, one of the defendants is alleged to have stolen proprietary and confidential designs and specifications for pipes for a nuclear power plant that Westinghouse Electric Company was contracted to build.[147] SolarWorld, a German solar product company operating in the United States, was also allegedly hacked by the defendants, and thousands of emails

---

03/11/world/asia/china-calls-for-global-hacking-rules.html [https://perma.cc/79VB-3YTF]; Mike Brownfield, *Morning Bell: Stopping the Cyber Espionage Threat*, DAILY SIGNAL (Apr. 26, 2012), http://dailysignal.com/2012/04/26/morning-bell-stopping-the-cyber-espionage-threat/ [https://perma.cc/AFJ6-NS3Y]; Michael Riley & Dune Lawrence, *Hackers Linked to China's Army Seen From EU to D.C.*, BLOOMBERG BUS. (July 26, 2012, 7:00 PM), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html [https://perma.cc/A9NS-CMLR]; Jody Westby, *Mandiant Report on Chinese Hackers Is Not News But Its Approach Is*, FORBES (Feb. 20, 2013, 8:07 AM), https://web.archive.org/web/20151010014944/http://www.forbes.com/sites/jodywestby/2013/02/20/mandiant-report-on-chinese-hackers-is-not-news-but-its-approach-is/.

[141] *See* Barboza, *supra* note 140.

[142] Terril Yue Jones & Benjamin Kang Lim, *China's New Premier Seeks "New Type" of Ties with U.S.*, REUTERS (Mar. 17, 2013, 4:02 AM), http://www.reuters.com/article/us-china-parliament-hacking-idUSBRE92G02320130317 [https://perma.cc/TZB8-3CXS].

[143] Claburn, *supra* note 119.

[144] *See* Zach West, *Young Fella, if You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 127 (2012).

[145] Indictment at 1–3, United States v. Dong, No. 14-00118 (W.D. Pa. May 1, 2014).

[146] *Id.* at 2.

[147] *Id.* at 4.

containing information such as cost structures and production capabilities were stolen.[148]

One of the defendants was also charged with using a tactic called "spear phishing" to obtain access to computers at U.S. Steel Corporation.[149] This involved sending an email message to an employee at U.S. Steel that was designed to trick the employee into allowing the defendant access to the company's computers.[150] Senior managers at Alcoa Inc., an aluminum manufacturer, were also targeted with spear phishing messages in an attempt to obtain trade secrets.[151] The spear phishing messages usually looked like emails from colleagues, and contained attached files or hyperlinks within the messages that, once opened, would install malware or malicious code onto the computer system, thus creating a "backdoor."[152] The defendants, acting as co-conspirators, tried to mask the identity and location of the computers from which they were operating their hacking activities by using "hop points," or computers belonging to other victims.[153]

3. Employees, Hackers, and RATs

Ironically, although companies are likely to believe that attackers and misappropriators will be hackers, foreign governments, competitors, and others outside of the company, the reality is that the biggest threat to company trade secrets has always been from the inside. Employees and others with access to the inside of the business are responsible for a large majority of trade secret theft, whether through cyber misappropriation or otherwise.[154] Misappropriation from insiders is also likely to be more costly[155] to companies.[156] Accordingly, as we continue to fight the battle in cybersecurity and to protect trade secrets, it is important to remember that building technological walls to defend against invaders and intruders is only part of the solution. Instead, even more careful consideration must be paid to the humans who are already inside of the

---

[148] *Id.* at 4–5.
[149] *Id.* at 6.
[150] *Id.*
[151] *Id.* at 7.
[152] *Id.* at 9.
[153] *Id.* at 9–10.
[154] *See, e.g.*, RANTALA, *supra* note 59,at 2 (reporting that in 2005, 75% of cyber thefts were due to business insiders).
[155] *See* COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., *supra* note 58, at 43 (detailing the crippling economic impact cyber attacks continue to have on U.S. companies).
[156] *See* Atul Gupta & Rex Hammond, *Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination*, 13 INFO. MGMT. & COMPUTER SECURITY 297, 299 (2004) (stating that while most organizations are focused on outside cyberattacks, misappropriation from the inside is harder to catch and costs companies more).

gates, and who are able and willing to use deception and other vices to obtain sensitive information.[157]

Several recent cases illustrate how humans and technology can be a perilous combination when it comes to keeping trade secrets safe. The former employees of an executive search firm allegedly used their usernames and passwords to copy and download trade secret information from a company database before leaving to start a competitive venture.[158] A government employee used his work computer to download and transfer files containing source code from the Citadel.[159] In another case, a Massachusetts employee on the verge of being terminated ordered his assistant in China to encrypt secret project files on the company's Chinese server.[160] The files were then condensed, password-protected, and sent to the employee at home, and the original files were destroyed.[161] This effectively blocked the company from accessing its own files after the defendant left because he refused to divulge the password.[162]

Competitors are often involved, either directly or indirectly, with alleged acts of cyber misappropriation. In one case, competitors accused each other of stealing electronically stored trade secrets, such as pricing and sales information, customer lists, and customer profiles.[163] The accused company in the case allegedly hacked into the plaintiff's computers and website, gaining access to passwords and login information with which it later obtained trade secrets.[164] Over a period of about three years, employees were also allegedly involved in supplying secret information to the competitor before leaving to join that competitor.[165]

One company allegedly induced a disloyal employee to steal proprietary financial modeling software from a competitor after the competitor had turned down an offer to purchase the company's business unit.[166] This employee was a trusted director of information technology at the company, and he allegedly accessed about 15,000 confidential computer files and emailed them to the competitor.[167] He also downloaded and copied the plaintiff's proprietary busi-

---

[157] *See* P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 65 (2014).

[158] United States v. Nosal, 930 F. Supp. 2d 1051, 1054–55 (N.D. Cal. 2013).

[159] United States v. Pu, 15 F. Supp. 3d 846, 852–53 (N.D. Ill. 2014).

[160] Enargy Power Co. v. Xiaolong Wang, No. 13-11348-DJC, 2013 U.S. Dist. LEXIS 170193, at *3 (D. Mass. Dec. 3, 2013).

[161] *Id.* at *3–4.

[162] *Id.* at *4.

[163] Big Rock Sports, LLC v. AcuSport Corp., No. 408-CV-159-F, 2011 U.S. Dist. LEXIS 110995, at *2 (E.D.N.C. Sept. 26, 2011).

[164] *Id.* at *7.

[165] *Id.*

[166] Charles Schwab & Co. v. Carter, No. 04-C-7071, 2005 U.S. Dist. LEXIS 5611, at *1–3 (N.D. Ill. Feb. 11, 2005).

[167] *Id.* at *3.

ness models onto a laptop for the benefit of the competitor and his soon-to-be new employer.[168]

Websites can be fair game as a source for trade secret misappropriation, as well. One company used the login name and password of a subscriber to its competitor's website in order to "sneak in" to view information available to the competitor's subscribers.[169] Its officers also allegedly hacked into the source code used by the competitor to operate its website, taking advantage of a back-door opportunity created by the competitor's failure to install a patch that had been distributed by Microsoft.[170] In another case, the defendant company and its employee allegedly hacked into a competitor's website by sending "electronic robots" to launch attacks and steal confidential source code and confidential customer information.[171] This kind of "extraction software" is used to search, copy, and retrieve information from websites.[172] The plaintiff was able to track the attacks to IP addresses tied to the defendant competitor.[173]

Hacking refers to a wide range of activities where a person intrudes upon or accesses a system belonging to another without the appropriate authorization.[174] Not only can computers be hacked, but virtually any other device or equipment that contains a computing system can also be vulnerable, such as cars, airplanes, and medical devices.[175] Indeed, right around the corner, the "Internet of things"—which is predicated on people being more connected to their devices—may leave consumers and trade secret owners even more vulnerable.[176] The digital components found in cars, insulin pumps, pacemakers, and even home refrigerators will provide more of a playground and greater opportunities for hackers.[177]

---

[168] *Id.* at *4.

[169] Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 932 (9th Cir. 2004).

[170] *Id.*

[171] Physicians Interactive v. Lathian Sys., No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *1–3 (E.D. Va. Dec. 5, 2003).

[172] *Id.* at *6.

[173] *Id.* at *5.

[174] *See* Leeson & Coyne, *supra* note 118, at 514.

[175] *See, e.g.*, Ralph Ellis, *Airplane Computer Systems Can Be Hacked, GAO Report Says*, CNN (May 18, 2015, 3:31 PM), http://www.cnn.com/2015/05/18/us/airplane-computer-hacking/ [https://perma.cc/L2JF-ZMM5]; Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/4D7U-VL9G].

[176] *See* Alex Wood, *The Internet of Things Is Revolutionising Our Lives, but Standards Are a Must*, The GUARDIAN (Mar. 31, 2015, 7:11 AM) (http://www.theguardian.com/media-network/2015/mar/31/the-internet-of-things-is-revolutionising-our-lives-but-standards-are-a-must [https://perma.cc/69RV-T2EH] (explaining that the term "Internet of things" was coined in 1999 to describe a future in which devices would be connected to each other and the Internet).

[177] *See* Lillian Ablon & Martin Libicki, *Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data*, 82 DEF. COUNSEL J. 143, 150 (2015).

Although insiders or employees can certainly be hackers,[178] the term in the context of trade secret misappropriation typically tends to refer to outsiders. For example, a citizen of Sweden was extradited to the United States after he was indicted on several counts of conspiracy to commit computer hacking.[179] He was the founder of an organization that developed malware, which included a remote access tool that could remotely control the victims' computers by capturing their keystrokes and searching through their files.[180] The RAT could also scan hard drives for other confidential information such as credit card numbers.[181] In 2014, there were highly publicized hacks at such well-known companies as Target, Home Depot, J.P. Morgan Chase, and Sony.[182] The kinds of information obtained from these hacks included not only consumer information like credit card information, but confidential, trade secret information as well.

There appears to be a thriving cybercrime market for this kind of trade secret information, and the kinds of tools that allow hacking are now widely and easily available.[183] Accordingly, gone are the days when only those with the highest computer programming skill levels could engage in this behavior. Today, one can hire a hacker or purchase exploit kits that contain all the software for creating and managing attacks.[184] It has also become the province of organized crime, perhaps in some ways easier and more lucrative than selling drugs.[185] The demographic characteristics of the typical hacker today suggests that person is likely to be male and under the age of thirty.[186] Hackers can include everyone from spies to dissatisfied employees, political activists, and even teenagers playing computer games.[187]

Hackers are not, however, all cut from the same cloth. Distinctions are being made between "good" hackers and "bad" hackers, or "ethical" hackers and "unethical" hackers. There is even a color-coding system for the various categories, with intent separating White Hats from Black and Grey Hats.[188] White

---

[178] *See* Henry Dalziel, *Motive and Motivation Are the ONLY Skills a Real Hacker Needs*, CONCISE BLOG (June 18, 2013, 1:22 PM), https://www.concise-courses.com/security/motive-and-motivation/ [https://perma.cc/9BF9-Y7ZJ] (explaining how employees have motive and motivation to hack their employers, especially when they are unhappy or resentful).

[179] United States v. Yücel, 97 F. Supp. 3d 413, 416–17 (S.D.N.Y. 2015).

[180] *Id.* at 416.

[181] *Id.*

[182] *See* Ablon & Libicki, *supra* note 177, at 143.

[183] *See id.* at 143–44.

[184] *See id.*

[185] *See id.* at 144.

[186] *See* Leeson & Coyne, *supra* note 118, at 516.

[187] *See* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 176 (2000).

[188] *See* CYNTHIA FITCH, SANS INST., CRIME AND PUNISHMENT: THE PSYCHOLOGY OF HACKING IN THE NEW MILLENNIUM 4–6 (2003), http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795 [https://perma.cc/MY7R-SDU3].

Hats tend to be security researchers who are hired to find security flaws.[189] Black Hats access systems to commit a crime, and Grey Hats are between the two, sometimes crossing the line in violating the law, but choosing to report security vulnerabilities.[190] Indeed, many hackers believe that unless their access is motivated by malicious intent, the practice should be legitimate.[191] The term "hacktivist" refers to those who hack for politically motivated reasons, trying to send a political message through a civil disobedience model.[192] Companies' trade secrets can be caught in the crossfire, as these hackers might seek to embarrass the company or harm its reputation.[193]

Some companies hire hackers or former hackers to test the vulnerabilities of their systems. This practice can be controversial.[194] Some argue that it provides the wrong incentives to hackers, in that it may serve as a pathway to landing a great job.[195] One could also question whether companies should trust "reformed hackers" with such access to their systems.[196] Some companies now offer "bug bounty programs," providing rewards to hackers who identify vul-

---

[189] *See* Kirsch, *supra* note 118, at 385.

[190] *See id*. Many Grey Hats are "reformed Black Hats now working as security consultants." FITCH, *supra* note 188, at 5.

[191] *See* Brent Wible, *A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577, 1590 (2003).

[192] *See* Tiffany Marie Knapp, *Hacktivism—Political Dissent in the Final Frontier*, 49 NEW ENG. L. REV. 259, 262 (2015) (describing hacktivism as the "nonviolent use of computer skills (or 'digital tools') for political purposes"); *see also* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 183 (2000) ("Hacktivists launch politically motivated attacks on public web pages or e-mail servers.").

[193] *See, e.g.*, Jessica Lavery, *Which Is More Dangerous: Cause-Motivated or Financially-Motivated Hackers?*, VERACODE (Feb. 27, 2015), http://www.veracode.com/blog/2015/02/which-more-dangerous-cause-motivated-or-financially-motivated-hackers [https://perma.cc/2TKY-TEBE].

[194] *See* Ki Mae Heussner, *Hacking Their Way to a Job?*, ABC NEWS (Apr. 17, 2009), http://abcnews.go.com/Technology/story?id=7356353&page=1&singlePage=true [https://perma.cc/5JJ6-LRE9].

[195] *See, e.g.*, Bas van den Beld, *Want to Work at Google? Hack Them and Leak!*, STATE OF DIGITAL (Aug. 30, 2011), http://www.stateofdigital.com/want-to-work-at-google-hack-them-and-leak/ [https://perma.cc/ZTY6-LBWP] (detailing how Google hired a hacker to avoid a leak of information); Alex Hern, *Yo Founder Apologises for Hack—And Hires One of His Hackers*, THE GUARDIAN (June 23, 2014, 5:59 AM), http://www.theguardian.com/technology/2014/jun/23/yo-founder-hack-hires-hackers-chat-app?CMP=twt_gu [https://perma.cc/S53X-XDD3] (discussing how the founder of Yo hired one of the app's hackers in order to prevent future breaches); Sara Yin, *7 Hackers Who Got Legit Jobs from Their Exploits*, PC MAG. (June 28, 2011), http://www.pcmag.com/slideshow/story/266255/7-hackers-who-got-legit-jobs-from-their-exploits [https://perma.cc/KM64-JP2C] (discussing Facebook's hiring of a former Sony hacker).

[196] *See* Leeson & Coyne, *supra* note 118, at 524.

nerabilities.[197] One of the many criticisms of the CFAA is that it captures and criminalizes all kinds of hackers, including legitimate security researchers.[198]

IV. Exploring Self-Help and Self-Defense

In the United States, there is no centralized government control or regulation of the Internet. Instead, the private sector, and in particular each company, is responsible for securing its own networks.[199] Companies cannot afford to rely on the government or on law enforcement to stem cyber misappropriation of their trade secrets. One drawback of the war rhetoric is that it might lead to an overreliance on the government to "fight the war," rather than focus on each company's ability and obligation to protect its own trade secrets. Under both the state civil law requirements and the EEA, putative trade secret owners must engage in reasonable efforts to protect confidential information before it receives the protected status of a trade secret. As will be discussed below, this sets the floor for a certain level of active efforts, appropriate to the circumstances, by which each company must act to guard its trade secrets.

The most likely source for trade secret misappropriation is still an insider, such as an employee or a business partner.[200] Even though cyber misappropriation from an outsider will be a less likely occurrence, these intrusions can be particularly damaging, especially if the attacker uses a sophisticated technique. For example, when employing an advanced persistent threat, the attacker breaches and lurks in the company's computer systems for months or years, monitoring activities and gathering information.[201]

Companies are right to fear and be concerned that the most significant losses might come from the outside.[202] This underscores the value and importance of protecting electronic data, engaging in self-help, and being proac-

---

[197] *See* Kirsch, *supra* note 118, at 397 (discussing bug bounty programs at Google, PayPal, and Facebook).

[198] *See id.* at 394–97; *see also supra* notes 61–70 (Part II.B, discussing how security researchers have faced legal action under the CFAA for exposing system vulnerabilities).

[199] *See* Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 Am. U. Bus. L. Rev. 225, 232–33 (2013) (discussing this "self-regulatory" approach to cybersecurity).

[200] *See* Peter J. Toren, *An Analysis of Economic Act Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!*, 84 Bloomberg BNA Pat., Trademark & Copyright J. 1, 5 (2012) (stating that the defendant was a company "insider" in over 90% of EEA prosecutions); *see also* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291, 303 (2010) (reiterating that the majority of misappropriations are committed by employees or business partners); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 Gonz. L. Rev. 57, 69 (2011) (stating that the thief was an employee or business partner in 93% of state cases and 90% of federal cases).

[201] *See* Alperovitch, *supra* note 87, at 2.

[202] *See* ASIS Int'l, Trends in Proprietary Information Loss 28, 33 (2007), https://foundation.asisonline.org/FoundationResearch/Publications/Documents/trendsinproprietaryinformationloss.pdf [https://perma.cc/YK78-WQNV].

tive in defending against all potential attacks through computers and the Internet, regardless of the source. It is also why relying solely on criminal laws or government policy to sufficiently protect individual businesses in the cat and mouse game of cyber misappropriation is an approach that will lead, at best, to unsatisfactory results without a self-help component. This Part will explore several initiatives, including self-help, self-defense, and government actions, as well as special considerations related to smaller companies, as they tend to be overshadowed and overlooked in discussions about cybersecurity and cyber misappropriation.[203]

A. Reasonable Efforts

In almost every state, the reasonable efforts requirement is embedded in the threshold legal question of trade secret misappropriation analysis: whether the plaintiff owns a legally protectable trade secret.[204] The Uniform Trade Secrets Act ("UTSA"), which has been officially adopted by forty-seven states and the District of Columbia,[205] includes reasonable efforts as part of the definition of a trade secret.[206] Reasonable efforts require that in order to qualify for trade secret protection, the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[207] The states that have not adopted the UTSA rely on the older codification of trade secret law in the *Restatement (First) of Torts*.[208] Even the *Restatement (First) of Torts*, however, requires a trade secret holder to show more than mere intent to protect something as a trade secret; actual effort to keep the information secret is necessary.[209] Thus, the *Restatement (First) of Torts* includes "the extent of measures taken by [the trade secret owner] to guard the secrecy of the information" as one of six factors to be considered in determining whether information qualifies as a trade secret.[210]

---

[203] *See infra* notes 304–313 and accompanying text (Part IV.D.1).

[204] *See* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELLECTUAL PROP. L. REV. 1, 6–7 (2007).

[205] *Legislative Fact Sheet—Trade Secrets Act*, UNIFORM LAW COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act [https://perma.cc/JTT5-LK82].

[206] UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005).

[207] *Id.*

[208] *See* JAMES POOLEY, TRADE SECRETS §§ 2.02[3], 2.04[3] (2015) (providing the *Restatement* rules and background information).

[209] *See* Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983) ("[E]ven under the common law, more than an 'intention' was required—the plaintiff was required to show that it had manifested that intention by making some effort to keep the information secret.").

[210] *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939). The remaining five factors are:

> (1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; . . . (4) the value of the information to [the business] and to [its] competitors; (5) the amount of ef-

Similar to the UTSA, the EEA also includes a reasonable efforts requirement in defining a trade secret.[211] The EEA requires that "the owner thereof has taken reasonable measures to keep such information secret."[212] This provision withstood a void for vagueness challenge in federal district court, with the court finding that the term "reasonable measures" is not unconstitutionally vague.[213] As a result, the showing of actual effort to preserve secrecy, required since codification of the *Restatement (First) of Torts*,[214] continues to be applicable under the EEA and in both UTSA and non-UTSA jurisdictions. The requirement is securely grounded in trade secret jurisprudence.

Although the above sources of law provide the underpinning for the reasonable efforts requirement, they do not provide precise standards for the courts on how to determine whether the requirement has been met.[215] The interpretation of the requirement appears to be similar in all jurisdictions such that for the purposes of this Article no further distinctions are necessary between UTSA and non-UTSA states. Whether a trade secret owner has utilized appropriate safeguards sufficient to meet the reasonable efforts requirement is a question of fact, based on the particular circumstances.[216] These decisions necessitate a balancing between using sufficient precautions to protect a company's secret on the one hand, without imposing overly burdensome precautions that would impair the functioning of its business on the other hand.[217] The inquiry necessarily calls for a cost-benefit analysis, which varies in each case based on the costs of the protective measures relative to the attendant benefits of protecting the information.[218] The costs to the trade secret owner will not only include direct financial costs, but also indirect costs, such as the ability to make appropriate use of the information in the business by sharing it with employees and others who need to use it.[219]

In the context of cyber misappropriation and cybersecurity generally, there is no such thing as an impenetrable fortress. Fortunately, the reasonable

---

> fort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Id.

[211] *See* 18 U.S.C. § 1839(3)(A) (2012).

[212] *Id.*

[213] *See* United States v. Hsu, 40 F. Supp. 2d 623, 628 (E.D. Pa. 1999) ("[A] statute is not void for vagueness merely because it uses the word 'reasonable' . . . .").

[214] Many courts, in both UTSA and non-UTSA jurisdictions, continue to rely on and cite to the *Restatement (First) of Torts*. *See* POOLEY, *supra* note 208, § 2.02[3] n.12.

[215] *See* Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 462 (1992).

[216] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 176–77 (7th Cir. 1991).

[217] *See id.* at 178–80.

[218] *See id.* at 179.

[219] *See id.* at 180.

efforts requirement does not mandate absolute secrecy.[220] "Rather, the standard is one of relative secrecy; a trade secret owner needs to take steps that are reasonably necessary under the circumstances to maintain secrecy."[221] A plaintiff in trade secret litigation must show that it took affirmative steps and concrete efforts to preserve the confidentiality of the alleged secret information.[222] Some courts note that in addition to requiring employees to sign confidentiality agreements, "reasonable efforts" can include "advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' . . . and keeping secret documents under lock."[223] Other reasonable efforts include "[t]he use of security guards, closed-circuit television monitors, access codes for information stored on a computer, and varying security access levels for different areas of the facilities."[224]

Efforts to protect secrecy are also tied to the requirement that trade secrets have value. Whether or not a company took adequate steps to protect a secret is considered evidence of the subjective belief that the information was a trade secret, and therefore worthy of protection.[225] For example,

> Some courts may reason that there is a direct relationship between the value of the information and the extent to which the company made efforts to protect it such that the more valuable the information to the company, the more costly or extensive the measures ought to be to protect it.[226]

---

[220] *See* 14 U.L.A. 538; *see also* Sheets v. Yamaha Motors Corp., 849 F.2d 179, 183–84 (5th Cir. 1988) (holding that Louisiana requires only reasonable efforts be taken to guard trade secrets); Comput. Assocs. Int'l v. Quest Software, Inc., 333 F. Supp. 2d 688, 696 (N.D. Ill. 2004) (noting that the Illinois Trade Secrets Act, which is based on the Uniform Trade Secrets Act, requires "reasonable measures, not perfection.").

[221] Rowe, *supra* note 7, at 9; *see also Sheets*, 849 F.2d at 183 ("[C]ourts do not require extreme and unduly expensive procedures be taken to protect trade secrets.").

[222] *See, e.g.*, Niemi v. Am. Axle Mfg. & Holding, Inc., No. 269155, 2007 WL 29383, at *4 (Mich. Ct. App. Jan. 4, 2007) (granting summary judgment in favor of defendant because plaintiff did not make actual efforts to preserve the confidentiality of the designs in question, such as marking the documents or requiring confidentiality agreements); Dicks v. Jensen, 768 A.2d 1279, 1284 (Vt. 2001) (granting summary judgment for defendant where there was "no evidence in the record that plaintiff took any measures to indicate that the customer list was confidential").

[223] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1253 (N.D. Cal. 1995) (citations omitted); *see* Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661, 693–94 (D. Minn. 1986) (discussing these precautions in detail), *aff'd*, 828 F.2d 452 (8th Cir. 1987).

[224] Rowe, *supra* note 7, at 10; *see* Schalk v. State, 767 S.W.2d 441, 447–48 (Tex. Ct. App. 1988) (detailing examples of security measures taken by the employer that the court considered), *aff'd*, 823 S.W.2d 633 (Tex. Crim. App. 1991) (en banc).

[225] *See* Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199–1200 (5th Cir. 1986) (reasoning that secrecy measures constitute evidence probative of the existence of a trade secret).

[226] Rowe, *supra* note 7, at 10; *see also* Jermaine S. Grubbs, Comment, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the "Reasonable Efforts" Taken by Small Businesses Should be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421, 426 (2005) ("The value of the

Furthermore, where a plaintiff makes a strong showing of reasonable efforts to protect trade secret information, a court is more likely to infer that the defendant improperly obtained the information.[227] But a trade secret owner who is lax about taking precautions to guard the secret cannot expect to prevent others from using it.[228] Thus, "a court may use the reasonable efforts requirement to deny a plaintiff any protection under trade secret law."[229] Even when a plaintiff creates a trade secret protection plan providing for how secrets will be safeguarded, a court could find, vis-à-vis the hypothetical reasonable person, that failure to adequately follow the plan is unreasonable conduct.[230]

B. Introducing TRAP

In order to effectively combat the kinds of remote access tools, or RATs, that can remotely control a victim's computer and access their files, it is necessary that companies take a more active stance to protect their trade secrets. Accessing remotely without needing to be on the same premises has opened up the world of potential perpetrators, setting up an unwieldy cat and mouse game. Accordingly, this Article introduces the acronym TRAP for "technologically responsive active protection" to serve as a guiding principle that further refines the reasonable efforts requirement for the protection of trade secrets. Consistent with every putative trade secret owner's duty to protect its trade secrets, rather than being passive in its efforts, TRAP reinforces the need to take initiative and be self-reliant in preparing and implementing security plans to protect against trade secret misappropriation through electronic means.

The enormous challenges that technology presents through the interconnected framework of the Internet raises the stakes in protecting proprietary information. The larger problem of cybersecurity and espionage is clearly a

---

information to the information holder and prospective appropriator will determine the amount of protection required.").

[227] *See* Grubbs, *supra* note 226, at 427; *see also Rockwell Graphic*, 925 F.2d at 179 ("The greater the precautions that [plaintiff] took to maintain the secrecy of the piece part drawings, the lower the probability that [defendant] obtained them properly and the higher the probability that it obtained them through a wrongful act . . . .").

[228] *See, e.g.*, Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1056–57, 1063 (2d Cir. 1985) (holding that defendant's use of a consumer list could not be enjoined because plaintiff did not take adequate measures to protect the information when selling its assets); Fisher Stoves, Inc. v. All Nighter Stove Works, Inc., 626 F.2d 193, 196 (1st Cir. 1980) (finding no misappropriation where competitor accidentally discovered customer data that plaintiff left behind); *see also* Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1445 (2009) ("Secrecy is the key to creating and preserving a trade secret. . . . [O]nce a trade secret becomes public, it can no longer be a trade secret and others are free to use it.").

[229] Rowe, *supra* note 7, at 10; *see, e.g.*, *Dicks*, 768 A.2d at 1284 ("It would be anomalous for the courts to prohibit the use of information that the rightful owner did not undertake to protect.").

[230] *See* Gemisys Corp. v. Phoenix Am., Inc., 186 F.R.D. 551, 558, 567 (N.D. Cal. 1999) (granting defendant summary judgment where plaintiff failed to use confidentiality legends pursuant to the terms of its license agreement).

matter of national concern, and a cooperative stance between the public and private sectors will always be essential. Nevertheless, each company must build its own fortress in this "war," rather than rely on external sources for protection. Active protection certainly requires consideration of technological tools. The use of such tools to protect, hide, or fight back must be considered. For example, some companies build fake networks, create fake documents, or build beacons into their documents that provide more information about who has taken property, not just that it was compromised.[231] Although many of these tools are considered passive, other more aggressive techniques are beginning to emerge as options. Hacking back is an example of an active defense mechanism, but one that is controversial. The nature of that controversy will be further explored later in this Part.[232]

Many companies do not invest sufficiently in cybersecurity and protecting their trade secret information.[233] Moreover, to the extent that a company's network may be interconnected with others, vulnerability can be shared on a larger scale as companies increasingly connect over the Internet.[234] Thus, guarding and protecting one's own secrets and assets has benefits beyond each individual company. The private sector can therefore, as a practical matter, play an important role in increasing security.

Companies may choose not to invest, or to invest minimally, in security for a host of reasons. The financial costs associated with shoring up networks and computers can be a deterrent, especially when for many companies the return on investment is uncertain.[235] This problem can be particularly acute with small businesses.[236] Not only are the financial costs more likely to be burdensome, but these businesses might be more likely to underestimate or

---

[231] *See* Stewart Baker, *Taking the Offense to Defend Networks*, STEPTOE CYBERBLOG (June 19, 2012), http://www.steptoecyberblog.com/2012/06/19/taking-the-offense-to-defend-networks/ [https://perma.cc/8GR2-TXV5].

[232] *See infra* notes 253–298 and accompanying text (Part IV.C).

[233] *See* Leon E. Panetta, Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 [https://perma.cc/3JD4-XJUP] ("Although awareness is growing, the reality is that too few companies have invested in even basic cybersecurity.").

[234] *See* Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, DAEDALUS, Fall 2011, at 70, 73 ("[The] lack of information about vulnerabilities, incidents, and attendant losses makes actual risk calculations difficult.").

[235] *See* Teplinsky, *supra* note 199, at 307 (explaining the lack of reliable data about the return on investment for cybersecurity).

[236] *See infra* notes 304–313 and accompanying text.

downplay their risks.[237] Small businesses are also less likely to have the kinds of internal policies in place to secure their information.[238]

Technologically responsive active protection encompasses the view that as a result of technology, trade secret protection has become far more difficult. As such, effective approaches must account for these technological advances, including the interconnectedness of all systems and the intangibility of the kinds of information that companies seek to protect. Accordingly, reasonable efforts to protect trade secrets in this context must be active and ongoing, and must integrate people and processes for optimal protection. Indeed, because the existence of technological controls might in itself create a false sense of security, it is imperative that the role of the people in implementing technological processes effectively be underscored.

Although much is made of the role of technological responses to combating trade secret misappropriation and other kinds of cyberattacks, the role of human behavior is largely overlooked despite its prevalence: "[H]uman error accounts for 35%–53.5% of cyber breaches caused by preventable employee error or sabotage from within a company in both the public and private sectors."[239] Another recent report found that over 60% of the electronic espionage cases in 2014 involved opening emails with malicious links or attachments.[240] Yet another report in 2014 places the number of security incidents attributable to human error at an even higher rate of 95%.[241] Apparently, it is such a sure thing that employees will open these kinds of emails that "sending emails to just ten employees will get hackers inside a corporation's system 90 per cent of the time."[242] So important is the role that employees play within any organization's security protection program that some companies, Lockheed Martin for instance, employ tactics such as tricking their employees into opening suspi-

---

[237] *See* Press Release, Symantec, New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans (Oct. 15, 2012), https://www.symantec.com/about/newsroom/press-releases/2012/symantec_1015_01 [https://perma.cc/5SPL-XNRG].

[238] *See* NAT'L CYBERSECURITY ALLIANCE & SYMANTEC, 2012 NATIONAL SMALL BUSINESS STUDY 4 (2012), https://staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf [https://perma.cc/ZV8B-T3BB] (finding that the majority of small business owners did not have an established Internet security policy in writing).

[239] Devin C. Streeter, *The Effect of Human Error on Modern Security Breaches*, STRATEGIC INFORMER: STUDENT PUBL'N OF THE STRATEGIC INTELLIGENCE SOC'Y, 2013, at 5, 6.

[240] Edd Gent, *Successful Hacks and Cyber Attacks Commonly Result of Human Error*, ENGINEERING & TECH. MAG. (Apr. 14, 2015), http://eandt.theiet.org/news/2015/apr/threat-reports.cfm [https://perma.cc/22QZ-VVQS].

[241] *See* Nicole van Deursen, *How to Reduce Human Error in Information Security Incidents*, SECURITY INTELLIGENCE (Jan. 13, 2015), https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/ [https://perma.cc/5CH7-F4T9] (citing the IBM Security Services 2014 Cyber Security Intelligence Index).

[242] Gent, *supra* note 240.

cious emails to help ensure that their message on security is actually being implemented.[243]

The reasons why employees misappropriate trade secrets, even without criminal intent, can be due to a wide range of factors, including complacency, apathy, ignorance, and stress.[244] But regardless of motivation, the primary line of defense in protecting trade secrets must account for employees and their human tendencies.[245] Accordingly, employees must be appropriately trained as well as informed about protecting the company's trade secrets and confidential information, and security procedures must be strictly enforced.

A well-considered security plan will include analysis of both internal and external risks, consider the nature of the trade secret information to be protected, appropriately tailor reasonable security measures to protect the sensitive information, and ensure ongoing assessment and review of the security plan in order to update what weaknesses appear.[246] Experts believe that even the most basic steps to protect against cyber intrusions could prevent about eighty percent of such attacks.[247] How money is spent is also of significance. For instance, it is best that companies do more than just protect against perimeter attacks generally designed to detect breaches, and become more aware of developing intelligence about threats.[248] It is also highly recommended that companies encrypt information so that even if it is stolen, it will have no value to the thief.[249]

Looking ahead, it will be interesting to see the role that insurance plays in encouraging companies to beef up their security. As companies purchase policies to reduce their expected losses from attacks, insurance companies will likely play a role in helping to develop best practices, as well as encouraging companies to adopt those practices to reduce their premiums or as a precondi-

---

[243] SINGER & FRIEDMAN, *supra* note 157, at 64–66.

[244] *See* DAVID LACEY, MANAGING THE HUMAN FACTOR IN INFORMATION SECURITY: HOW TO WIN OVER STAFF AND INFLUENCE BUSINESS MANAGERS 52–53 (2009).

[245] *See* Munir Ahmed et al., *Human Errors in Information Security*, 1 INT'L J. ADVANCED TRENDS COMPUTER SCI. & ENGINEERING 82, 82–83 (2012).

[246] The Federal Trade Commission has made similar recommendations for the protection of consumer information. *See* Hiller & Russell, *supra* note 38, at 239.

[247] *See, e.g.*, Howard A. Schmidt, *Price of Inaction on Cybersecurity Will Be the Greatest*, N.Y. TIMES (Oct. 18, 2012, 6:13 AM), http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest [https://perma.cc/VG26-QFQ7] ("It is estimated that as high as 85% of successful intrusions could have been prevented by just implementing good 'cyber-hygiene.'").

[248] *See* Tsion Gonen, *Breach Prevention Is Dead. Long Live the 'Secure Breach,'* NETWORK WORLD (Oct. 29, 2012, 5:48 PM), http://www.networkworld.com/article/2161056/tech-primers/breach-prevention-is-dead--long-live-the--secure-breach-.html [https://perma.cc/SE5F-QLHW] (providing steps for a more realistic and effective response to perimeter breaches).

[249] *See, e.g., id.* (discussing a breach involving Zappos, where encrypted information was accessed but of no value to the attacker).

tion to coverage.[250] This might serve as a motivating factor for companies to invest in technological and other tools to protect against misappropriation. The best security plans must also account for human error, recognizing that even the smartest technological tools can be undermined by human behavior.[251] Although this Part so far has discussed technological tools generally as one large grouping, the next section[252] separates out passive tools from the more controversial active defense tools, illustrating that choices for active protection lie along a spectrum.

C. Active Defense and Hacking Back

Defensive measures to computer security include firewalls, encryption, automated detection of intrusions, and education of employees and users of computer systems.[253] In the parlance of cybersecurity, these are considered passive measures.[254] Somewhere between these passive measures and more active defense measures are approaches that, for instance, use decoy sites to attract hackers. These are known as "honeypots."[255] Honeypots can be created to work as traps to capture information about intrusions.[256] One limitation of honeypots is that they only work when there has been direct communication from an attacker.[257] Another method known as a "sandbox" isolates execution of code to help better protect the integrity of an entire system that may be infected with malicious code.[258] A limitation of this approach is that the sandbox could be bypassed.[259] Accordingly, some commentators believe that reliance

---

[250] *See* Walter S. Baer & Andrew Parkinson, *Cyberinsurance in IT Security Management*, IEEE SECURITY & PRIVACY, May/June 2007, at 50, 50–51.

[251] *See* Kirsch, *supra* note 118, at 395.

[252] *See infra* notes 253–298 and accompanying text (Part IV.C).

[253] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 450 (2012).

[254] *See id.*

[255] *See* Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 53 (2005) (explaining that honeypots are "decoy sites designed to look like promising targets to hackers").

[256] *See* LANCE SPITZNER, HONEYPOTS: TRACKING HACKERS 23 (2003); Laurent Oudot & Thorsten Holz, *Defeating Honeypots: Network Issues, Part 1*, SYMANTEC (Jan. 7, 2015), http://www.symantec.com/connect/articles/defeating-honeypots-network-issues-part-1 [https://perma.cc/A4J7-4N9P].

[257] *See* Lance Spitzner, *Honeypot Farms*, SYMANTEC (Nov. 2, 2010), http://www.symantec.com/connect/articles/honeypot-farms [https://perma.cc/9SVB-X4PM] (acknowledging this weakness but advocating for the significant potential of honeypots to defend against cyberattacks).

[258] *See* Dan Goodin, *Chrome Is the Most Secured Browser—New Study*, THE REGISTER (Dec. 9, 2011, 1:45 PM), http://www.theregister.co.uk/2011/12/09/chrome_ie_firefox_security_bakeoff [https://perma.cc/5FJQ-NVGS] ("[S]andboxes are designed to lessen the damage attackers can do when they successfully exploit a vulnerability in the underlying code base.").

[259] *See* Robert Westervelt, *Researcher Breaks Adobe Flash Sandbox Security Feature*, TECHTARGET (Jan. 6, 2011), http://searchsecurity.techtarget.com/news/1525813/Researcher-breaks-Adobe-Flash-sandbox-security-feature [https://perma.cc/UY2T-K4DZ].

on passive defense features alone are insufficient for optimum protection,[260] and others consider honeypots and sandboxes to be active defenses rather than passive.[261]

On the other end of the spectrum from passive defense mechanisms are active defenses. More active and offensive measures are beginning to emerge as companies become more proactive against hacking. An active defense allows a company to detect an intrusion, trace it, and actively respond to the threat. This could include interrupting an attack in progress in order to lessen the damage that it may cause, all the way to counter-striking the attacker.[262] The technique of beaconing is also an active defense technique that, when attached to an electronic file, alerts when it has left an authorized network and also potentially identifies its location in the event it is stolen.[263] Other versions of this type of decoy or trap on files to detect attacks include techniques known as "web bugging," "meta-tagging,"[264] and "watermarking."[265] Another more aggressive approach might be inserting code into confidential files so that if stolen, the data would self-destruct.[266] New business models are also emerging to assist corporations in dealing with the problem. Innovative companies are developing technology to assist companies in their defense against online threats. CrowdStrike, Endgame, and CloudFare are examples of startups entering this market.[267]

1. The Hacking Back Controversy

The pursuit of active defense is currently very controversial.[268] This is so for legal, technical, and political reasons. There are those who argue strongly in favor of this approach and those who oppose it. The larger debate in this area is usually about cyberattacks generally, including not just businesses but public infrastructure, wider national security issues, and international implications.[269] Continuing to draw on the war rhetoric in this area, active defense in

---

[260] *See, e.g.*, Kesan & Hayes, *supra* note 253, at 471–72.

[261] *See* McGee et al., *supra* note 95, at 11–12.

[262] *See* Kesan & Hayes, *supra* note 253, at 474–75.

[263] *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 1, 9 (2014).

[264] *Id.*

[265] McGee et al., *supra* note 95, at 30.

[266] *See* Christopher M. Matthews, *Support Grows to Let Cybertheft Victims "Hack Back,"* WALL STREET J. (June 2, 2013, 9:33 PM), http://www.wsj.com/articles/SB10001424127887324682204578517374103394466 [https://perma.cc/9MCA-KQB9].

[267] *See Firewalls and Firefights*, THE ECONOMIST (Aug. 10, 2013), http://www.economist.com/news/business/21583251-new-breed-internet-security-firms-are-encouraging-companies-fight-back-against-computer [https://perma.cc/9NE2-DUCC].

[268] *See infra* notes 295–298298 and accompanying text.

[269] *See, e.g.*, Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 162–67 (2005) (discussing defensive

military terms refers to "[t]he employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[270] Interestingly, however, the White House and the Department of Defense have not adopted the uniform definition for "active defense" in the context of cybersecurity.[271] In technical and legal circles, the phrase generally refers to the use of technology to respond directly to attacks.[272] The Justice Department's position is that companies should not hack back into an attacker's computer.[273] Since this Article focuses specifically on trade secrets, it will not engage in that wider debate.

In 2010, a group from China allegedly hacked into Google's network and those of many other U.S. companies.[274] Not only did Google successfully trace the source of the attack, but it also engaged in a counter-offensive move to obtain evidence about the culprits.[275] This has come to be known as "hacking back."[276] Google is not alone among large companies that are beginning to retaliate or respond to hacking in this manner.[277] Another Fortune 500 company

---

countermeasures in cyberwarfare between countries); *see also* Kesan & Hayes, *supra* note 253, at 520–25 (addressing domestic and international legal concerns with cyber self-defense); Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 189–94 (2005) (applying principles of tort law to cyber self-defense practices).

[270] *See* JOINT CHIEFS OF STAFF, JOINT PUB. NO. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 1 (Nov. 8, 2010, as amended through Jan. 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf [https://perma.cc/7U7D-3XTR].

[271] *See* Ellen Nakashima, *When Is a Cyberattack a Matter of Defense?*, WASH. POST (Feb. 27, 2012), http://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html [https://perma.cc/KJ7P-A3JT] (noting discord between the White House and the Department of Defense as to the definition of the term).

[272] *See* Joseph Menn, *Hacked Companies Fight Back with Controversial Steps*, REUTERS (June 18, 2012, 11:53 AM), http://www.reuters.com/article/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618 [https://perma.cc/3T3A-55PJ].

[273] *See* Rosenzweig, *supra* note 89, at 115–16.

[274] *See* Riva Richmond, *Flawed Security Exposes Vital Software to Hackers*, N.Y. TIMES: BITS (Mar. 5, 2010, 7:04 PM), http://bits.blogs.nytimes.com/2010/03/05/flawed-security-exposes-vital-software-to-hackers/ [https://perma.cc/4ZSS-NUMR].

[275] *See* Ellen Nakashima, *U.S. Plans to Issue Official Protest to China Over Attack on Google*, WASH. POST (Jan. 16, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/01/15/AR2010011503917.html [https://perma.cc/2QSF-S6HW]; David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 15, 2010), http:// www.nytimes.com/2010/01/15/world/asia/15diplo.html [https://perma.cc/RTY8-75XB].

[276] *See* Matt Buchanan, *Google Hacked the Chinese Hackers Right Back*, GIZMODO (Jan. 15, 2010, 10:32 AM), http://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back [https://perma.cc/2W94-D53X].

[277] *See, e.g.*, *Firewalls and Firefights*, *supra* note 267; Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law & Legal Theory Papers Series, Research Papers Series No. 08-20, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932 [https://perma.cc/DM52-YMK7] (citing a study that found 30% of Fortune 500 companies had installed counterattack software); *see also* Menn, *supra* note 272 (discussing the growing trend of U.S. companies conducting retaliatory hacking); James Temple, *Hackers Getting Hacked by*

also allegedly used software that slowed an intrusion and blocked the hacker's computer from the company's website.[278] It is believed that more companies will pursue this option.[279] The full extent of these measures, as used by companies currently, are and will likely remain unknown.[280] For one thing, firms generally do not publicly disclose that they are engaging in this behavior for much the same reason that they keep private when they have been hacked.[281] Potential negative questions or publicity associated with hacking back might also serve to discourage such public announcements.[282] These measures no doubt remain controversial.[283]

When a company hacks back it mounts a counterattack against its attacker, often trying to damage the perpetrator's system. There are various ways to do this, some of which might include trying to overload the servers from which the attack originated in an attempt to prevent them from continuing the intrusion, or directly hacking into the servers responsible for the original attack.[284] One of the goals of the strategy is to de-incentivize and deter hackers while also improving corporate security. Some argue, however, that the deterrence effect is of limited use.[285] This kind of active defense strategy presents an opportunity to respond quickly to attacks, and some believe that, among other reasons, they may serve to deter hackers by increasing costs to them.[286]

Nevertheless, the approach is not without its shortcomings and potential pitfalls. There is a chance, for instance, that these kinds of counterstrikes might miss their targets and hit the wrong ones, thereby harming innocent third parties.[287] Attackers can also disguise their location so that a counterstrike affects a third-party and not the perpetrator.[288] Attackers often "spoof" their IP ad-

---

Security Firms, SFGATE (Nov. 30, 2011, 4:00 AM), http://www.sfgate.com/business/article/Hackers-getting-hacked-by-security-firms-2306472.php [https://perma.cc/HP5B-LNDW] (describing how some security firms are becoming more aggressive and effectively hacking the hackers themselves).

[278] *See* Temple, *supra* note 277.

[279] *See* Brian Prince, *Black Hat: Hacking Back—The Best Defense May Not Be the Best Offense*, SECURITY WK. (July 27, 2012), http://www.securityweek.com/black-hat-hacking-back-best-defense-may-not-be-best-offense [https://perma.cc/R28A-45C4] (discussing a survey that demonstrated a significant number of companies had conducted retaliatory hacks).

[280] *See* Kesan & Hayes, *supra* note 253, at 470.

[281] *See* Majuca & Kesan, *supra* note 277, at 2.

[282] *See* BRIAN CASHELL ET AL., CONG. RESEARCH SERV., RL32331, THE ECONOMIC IMPACT OF CYBER-ATTACKS 13–14 (2004).

[283] *See, e.g.*, Menn, *supra* note 272.

[284] *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1564 (2013).

[285] *See infra* notes 291–296 and accompanying text.

[286] *See Firewalls and Firefights*, *supra* note 267.

[287] *See, e.g.*, Curtis E. A. Karnow, *Launch on Warning: Aggressive Defense of Computer Systems*, 7 YALE J.L. & TECH. 87, 93 (2005); Katyal, *supra* note 255, at 62.

[288] *See, e.g.*, Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J.L. ECON. & POL'Y 197, 205 (2005).

dresses in order to evade detection.[289] Thus, a strike back against the apparent origin of the attack might harm an innocent victim whose computer was used as a "zombie" by the hacker.[290] Another concern is that private companies' responses might be excessive or disproportionate as they eagerly pursue a retaliatory objective.

2. Legal Implications

Some of the complicated issues around hacking back or retaliatory cyberattacks include the legal implications and ability of this method to serve as an effective deterrent. It is unclear whether this behavior is legal, but it is evident that better guidelines will be needed to address when such activities are legitimate and which should be sanctioned. For instance, such conduct may violate the CFAA.[291] On the international level, there are also questions about state-to-state engagement, and conduct between private individuals or companies across borders.[292]

Consistency among definitions, beginning with what constitutes a cyberattack, would also be necessary. Cyberattacks tend to refer to "the use of deliberate actions . . . to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks."[293] Perhaps more applicable to trade secrets, the term "cyber exploitations" often refers to actions that are not constructive, but that nonetheless remove confidential information from a network.[294] Nevertheless, the terms are often conflated with a cyberattack, referring to intrusions upon a network.

In any case, regardless of the terminology, counterstrikes like hacking back are highly controversial and potentially violate the CFAA.[295] Even those who favor the use of this kind of self-defense caution that more study and reg-

---

[289] *See* Matthew Tanase, *IP Spoofing: An Introduction*, SYMANTEC (Nov. 2, 2010), http://www.symantec.com/connect/articles/ip-spoofing-introduction [https://perma.cc/TA9P-73F2] ("In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by 'spoofing' the IP address of that machine.").

[290] *See* Smith, *supra* note 269, at 180.

[291] *See* 18 U.S.C. § 1030 (2012) (prohibiting unauthorized access to "protected" computers); *see also* Stewart Baker et al., *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ [https://perma.cc/P963-YSTY] (debating the legality of cyberhacking under the CFAA).

[292] *See, e.g.*, Messerschmidt, *supra* note 95, at 313–23; *see also* Kesan & Hayes, *supra* note 253, at 510–12 (discussing "the implications of international law for cybersecurity issues").

[293] *See* COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (William A. Owens et al. eds., 2009).

[294] *See id.* at 10–11.

[295] *See, e.g.*, Harrington, *supra* note 263, at 21–26; Katyal, *supra* note 255, at 61; Kesan & Hayes, *supra* note 253, at 520; Sales, *supra* note 284, at 1565–66; Smith, *supra* note 269, at 182; West, *supra* note 144, at 138.

ulation may be required in order to establish appropriate guidelines for legitimate use of counterstrikes that minimize collateral damage.[296] On some level, the practical reality suggests that any prosecution for this kind of behavior would be highly unlikely unless an innocent victim files a complaint or notifies law enforcement, especially since the hackers themselves will not be alerting law enforcement.

In drawing the appropriate lines, fine distinctions might be necessary to better match the legal ramifications with the technology. Questions abound. Which of these would be acceptable: destroying the attacker's system, limiting their bandwidth, and/or attaching a "beacon" to confidential files to allow notice when the file has left the authorized network and potentially identify the location of the file if it is stolen?[297] Should companies receive immunity for counterstrikes against hackers? Is striking against an attack analogous to self-defense? Is it analogous to the "stand your ground" doctrine in criminal law?[298] All of these are questions that need further and deeper exploration as legislators and policymakers continue the debate and wrestle with this difficult area.

D. Education and Supplementary Initiatives

As we await resolution and answers on these active defense questions from policymakers in courts, it may be that one of the best ways to address cyberattacks generally, and cyber misappropriation specifically, is through education. In the longer term, educating children about cybersecurity and safe practices, in addition to developing an appreciation for the protection of trade secrets and intellectual property rights, can be a supplementary and complementary approach to the larger national issues in this area. Working toward a cultural shift in the way we think about cybersecurity can have the most lasting effect. In the short-term, educating small businesses is also critical.

As technology has become part of the fabric of the current culture in which children are raised, it is worth paying attention to the moral and legal norms that surround how technology is and should be used. Researchers have found that when one's peer group is involved in computer crime, this encourages others in the group to do the same.[299] Accordingly, there is a role for education to help shape socially acceptable and legally acceptable behaviors and norms in teaching children about access to computers.[300] Thus, to the extent

---

[296] *See* Kesan & Hayes, *supra* note 253, at 535–37 (arguing that a public-private partnership should be developed to regulate active defense and counterstriking).

[297] *See* Harrington, *supra* note 263, at 9.

[298] *See Recent Developments—Florida Legislation*, 33 FLA. ST. U. L. REV. 351, 355 (2005) (discussing the Florida law that allows one to legally use force in self-defense without a duty to retreat).

[299] *See* FITCH, *supra* note 188, at 11–12.

[300] *See id.* at 13.

that hacking is seen as part of the fun and games attendant with technology, children and young adults must be taught what behaviors are legally acceptable and which are not. This is likely to help shape the collective consciousness over the long-term. To the extent that part of the attraction of hacking and other such activities is due to curiosity[301] and a sense of competition, educators may want to consider creating environments in which students can build on these skills in an appropriate educational framework.[302]

Further, developing a greater understanding of the harm and costs to victims—as well as a respect for trade secrets and other proprietary information—can go a long way to educate the public, particularly those that are not criminally motivated in the first place. For instance, there are those who believe that unless an intrusion is maliciously motivated, it is not unethical or illegal.[303] This is the kind of thinking that needs to be adjusted.

1. Small Companies

The larger discussions and voices around hacking, cyber misappropriation, and trade secret protection often are or make reference to large, well-known companies.[304] The significance and implications for smaller companies also deserve attention, as a thorough exploration of this issue would be remiss without consideration of small companies. Indeed, trade secret law, because of its initial low cost to entry and lack of government formalities to obtain its protections, is widely used and heavily relied upon by small businesses.[305] Ironically, they are also the entities that are probably less likely to be willing to expend large sums of money on reasonable efforts to protect their trade secrets. Nor are they likely to have the same level of access to attorneys and other advisors (including internal IT departments) to advise them of the importance of protecting their trade secrets in general and defending against cyber misappropriation in particular.

According to a recent report from Symantec, about sixty percent of cyberattacks in 2014 were aimed at small[306] and medium-sized businesses.[307]

---

[301] *See* LARISA APRIL LONG, SANS INST., PROFILING HACKERS 4 (2012), http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 [https://perma.cc/AQH6-57JW] (discussing hackers playing around to test possibilities and hone their skills).

[302] *See* FITCH, *supra* note 188, at 14.

[303] *See* Wible, *supra* note 191, at 1590.

[304] *See* Rosalie L. Donlon, *Small, Mid-Sized Businesses Hit by 62% of All Cyber Attacks*, PROP. CASUALTY 360 (May 27, 2015), http://www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber?page_all=1 [https://perma.cc/M6BG-SECL] (noting that in contrast to what is covered by the press, the majority of breaches are committed against local companies).

[305] *See* Grubbs, *supra* note 226, at 440.

[306] Note that there is some level of inconsistency among various reports on how small businesses are defined. Some consider the number of employees; others consider revenue. The precise definition is not significant for the purposes of this Article. For the purposes of trade secret misappropriation,

This represented an increase of about thirty percent from the previous year.[308] It suggests that not only are these businesses themselves at risk, but other companies with which they do business are also at risk, especially when the smaller business partner has its systems connected to those of the larger entity. The vulnerability can create a back-door access to proprietary information, placing the entire supply chain at risk.[309]

Smaller companies may suffer from the misconception that they are not fruitful targets for cyberattackers, and as such may not be willing, or sometimes simply not financially able, to invest sufficiently in securing their confidential information.[310] Instead, these companies tend to rely on antivirus protection as their defensive stronghold.[311] As a result of not paying enough attention to their security, however, they make themselves easier targets, placing the sensitive information belonging to those with whom they do business (both businesses and consumers) at even greater risk.[312] In addition to limited budgets and expertise to implement comprehensive security protocols, small businesses often are not as aware of the risks, and do not train their employees to identify risks or to engage in safer conduct.[313] Although they cannot be expected to have the same level of complex systems in place as larger entities, smaller businesses still must engage in reasonable efforts (that best match the enterprise) to protect their trade secrets. Accordingly, educating and raising awareness among this large and most vulnerable segment of trade secret owners is critical.

2. Government Initiatives

Law enforcement itself is also resorting to technological tools in the fight against cyber espionage. In September 2013, the Department of Justice recommended an amendment to Rule 41 of the Federal Rules of Criminal Proce-

---

however, this author conceptualizes a small business as having fewer than 100 employees. *Cf.* Gupta & Hammond, *supra* note 156, at 297–310 (conducting an empirical study of cybersecurity issues with regard to small businesses, and providing suggestions for future planning and improvement).

[307] SYMANTEC, *supra* note 35, at 6.

[308] *See id*. at 7 (providing this statistic for medium-sized business; the figure is 26% for small businesses).

[309] *See id*. at 70.

[310] *See* PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD 8 (2014), http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf [https://perma.cc/66QF-DZWC].

[311] *See, e.g.*, Debasis Bhattacharya, *Leadership Styles and Information Security in Small Businesses*, 19 INFO. MGMT. & COMPUTER SECURITY 300, 305 (2011).

[312] *See Combating Small Business Security Threats: How SMBs Can Fight Cybercrime*, MCAFEE (2012), http://www.mcafee.com/us/resources/white-papers/wp-combating-smb-threats.pdf [https://perma.cc/AW5W-M6KK].

[313] *See* Taylor Armerding, *Why Criminals Pick on Small Business*, CSO ONLINE (Jan. 12, 2015, 4:04 AM), http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html [https://perma.cc/F2F7-FX6D].

dure that would expand the territorial limits for searching electronic data.[314] In effect, this would authorize courts to issue warrants that would be executed by remotely accessing computers located outside the district where the court is located. The idea is that it would allow law enforcement to investigate crimes involving botnets and other anonymizing technologies used in cybercrime. Under the proposed amendment to Rule 41,

> Law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.[315]

Although this certainly might make it easier to conduct investigations, both domestically and internationally, the propriety of these programs used to conduct remote searches will raise constitutional and territorial questions.[316]

To the extent that government regulatory agencies have begun to mandate reporting or greater security within companies, this could also serve to encourage further investment in security. For instance, the Securities and Exchange Commission ("SEC") issued guidance in October 2011 requiring companies to report "material information regarding cybersecurity risks and cyber incidents."[317] Such disclosures are also tied to the relevant insurance coverage. Those two forces, insurance in the private marketplace coupled with governmental regulation, might provide other ways to incentivize at least those companies within the SEC's reach.[318]

The Obama Administration is also considering amending the Racketeer Influenced and Corrupt Organizations Act to include computer fraud: a move that would mean significant increases in penalties.[319] The Cyber Intelligence

---

[314] *See* Letter from Mythili Raman, Acting Assistant Attorney Gen., to the Honorable Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 1 (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [https://perma.cc/Y2VX-6FUS].

[315] *Id.* at 5.

[316] *See* Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1238–40 (2012) (discussing whether such investigative techniques would be considered a search under the Fourth Amendment).

[317] *See CF Disclosure Guidance: Topic No. 2*, SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://web.archive.org/web/20160209083337/http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[318] *See* Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG BUS., (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/articles/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure [https://perma.cc/TF8J-QTL5].

[319] *See Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyber Space and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) (statement of James A. Baker, Associate Deputy Attorney Gen., U.S. Dept. of Justice).

Sharing and Protection Act, which was passed by the House of Representatives in April 2013, included an amendment that did not permit hacking back.[320] But the Cybersecurity Information Sharing Act of 2014, designed to enhance and provide protections from liability for sharing of information between private corporate entities and the government, was passed out of the Senate Intelligence Committee.[321]

3. Approaches Outside the United States

Because challenges related to cybersecurity are occurring on a global scale, it is no surprise that the governments of many countries have undertaken plans and initiatives to address them. Along with the United States, among the countries taking serious note are Canada, Germany, Israel, the Netherlands, and the United Kingdom.[322] The United States is arguably the leader in thinking about and attempting to integrate cybersecurity in both the political and business sphere.[323] With respect to the use of self-defense measures by the private sector, there is no general consensus (as of yet) on the issue. There is a proposal in the Netherlands to permit law enforcement officials to hack internationally, but the proposal does not discuss private parties.[324] Similarly, Israeli Defense forces have the right to use "offensive cyber operations," but Israel takes no position on whether those in the private sector are permitted to do so.[325] In Germany, however, it is illegal to hack back.[326] Nevertheless, German companies have reportedly used hacking back, and the practice appears to be tolerated.[327] Countries are likely to approach this complicated issue in different ways to account for their unique cultural, government, and business sector concerns. The European Union, for instance, appears to be taking the approach of implementing mandatory standards, whereas the United States has tended more toward self-regulation.[328] Moving forward, there is a need to build a con-

[320] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

[321] Press Release, Dianne Feinstein, U.S. Senator, Senate Intelligence Committee Approves Cybersecurity Bill (July 8, 2014), http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=4C0EE3F0-8191-410C-B35D-BFE3BB0B3B46 [https://perma.cc/4NLW-2C8L].

[322] *See* Daniel Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH. 435, 438–39 (2015).

[323] *See* Jarno Limnell, *Europe Lags Behind US, China and Russia in Cybersecurity Race*, INT'L BUS. TIMES (July 13, 2015, 11:28 AM), http://www.ibtimes.co.uk/europe-lags-behind-us-china-russia-cybersecurity-race-1510627 [https://perma.cc/2G5R-S4XP].

[324] *See* Rosenzweig, *supra* note 89, at 114.

[325] *See id*.

[326] *See id*.

[327] *See, e.g.*, Ulrich Clau, *Hack Back—When a Cyber Attack Victim Turns 'Digital Vigilante,'* WORLDCRUNCH (July 21, 2012), http://www.worldcrunch.com/hack-back-when-cyber-attack-victim-turns-digital-vigilante/tech-science/hack-back-when-a-cyber-attack-victim-turns-digital-vigilante-/c4s5887/ [https://perma.cc/U492-WYMB].

[328] *See* Hiller & Russell, *supra* note 38, at 245.

sensus on these kinds of active self-defense measures, both within the private sector and between nations.

CONCLUSION

This Article has undertaken the formidable task of exploring cyber misappropriation and espionage within the larger problem of cybersecurity in the United States. Recognizing the significance of economic espionage to our national economy and national security, the government has embraced the rhetoric of war to frame the larger debate. This Article cautions that companies ultimately must look inward and re-conceptualize their roles, not as bystanders or onlookers, but as participants responsible for building their own TRAPs and fortresses to protect their trade secrets and proprietary information. Reliance on legislative and judicial intervention and enforcement alone will never be enough to offer adequate protection in a world where technologies, like RATs, permit easy access to American companies' trade secrets from anywhere in the world. Self-help is the first line of defense, without which the "war" cannot be won. Using TRAP as a guiding principle, companies may need to implement a layered security system that covers personnel as well as technology in order to mitigate risks. Even though perfect security is impossible to achieve, active protection can serve to lower risks of trade secret misappropriation through cyber misappropriation.