PROACTIVE CYBERSECURITY:
A COMPARATIVE INDUSTRY AND REGULATORY ANALYSIS

Amanda N. Craig, JD*, Scott J. Shackelford, JD, PhD**, & Janine S. Hiller, JD***

ABSTRACT

This Article analyzes recent business realities and regulatory trends shaping the proactive cybersecurity industry. To provide a framework for our discussion, we begin by describing the historical development of the industry and how it has been shaped by the applicable law in the United States and other G8 nations. We then catalogue the proactive cybersecurity practices of more than twenty companies, focusing on four case studies that we consider in the context of polycentric "global security assemblages." Finally, we assess the emergence of proactive cybersecurity norms, both within industry and international law, and consider the implications of this movement on contemporary Internet governance debates about the role of the public and private sectors in regulating cyberspace. Ultimately, we maintain that proactive cybersecurity, especially if pursued with improved legal clarity and global cooperation, demonstrates an opportunity for polycentric partnerships to result in better protected IT assets.

TABLE OF CONTENTS

INTRODUCTION

In January 2015, as Sony Pictures struggled to revive its computer network after *The Interview* reportedly prompted a massive hack,[1] cybersecurity firm FireEye demonstrated that the sorts of breaches that Sony experienced likely are not preventable with conventional network defenses.[2] Indeed, while experts said that "Sony's reputation is suffering" due to the hack, they also agreed that Sony "is hardly the only company at risk . . . ."[3] Rather, FireEye likens traditional network defense tools, on which Fortune 500 companies spent much of their $71 billion information technology ("IT") security budgets in 2014,[4] as something akin to France's pre-World War II "Maginot Line"—good in theory, but relatively easy to bypass in practice.[5] Recent news headlines may seem evidence enough, as Target, Home Depot, and J.P Morgan Chase all announced major breaches in 2014.[6] But FireEye's January 2015 report goes much further, noting that a whopping 96 percent of the 1,600 computer networks that it monitored—from *behind* traditional network defenses—were breached in 2014.[7] As such, FireEye argues, "organizations must consider a new approach to securing their IT assets . . . [they] can't afford to

The authors wish to thank Professors Amy Zegart, Larry Kramer, and Tiny Cuellar for their invaluable comments on this Article, as well as the research support of Scott Russell and Jonathan Brown. Scott in particular took the lead in developing the UK and Singapore case studies, for which we are indebted to him. The views expressed in this article are solely those of the authors and do not necessarily represent or reflect the position of Microsoft Corp.

* Senior Cybersecurity Strategist, Microsoft Corporation. *Disclaimer: The views expressed in this article are solely those of the author and do not necessarily represent or reflect the position of Microsoft Corporation.*
** Assistant Professor of Business Law and Ethics, Indiana University; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University.
*** Professor of Business Law, Richard E. Sorensen Professor in Finance, Pamplin College of Business, Virginia Tech.

[1] Thomas Halleck, *Sony Corporation: Network is Still Down Following 'The Interview' Hack*, INT'L BUS. TIMES (Jan. 8, 2015), http://www.ibtimes.com/sony-corporation-network-still-down-following-interview-hack-1778344; Dara Kerr and Roger Cheng, *Sony CEO: We were the victim of a vicious and malicious hack*, CNET (Jan. 5, 2015), http://www.cnet.com/news/sony-announces/.

[2] *Maginot Revisited: More Real-World Results from Real-World Tests*, FIREEYE (2015), https://www2.fireeye.com/rs/fireye/images/rpt-maginot-revisited.pdf [hereinafter *Maginot Revisited* (2015)].

[3] John Guadiosi, *Why Sony Didn't Learn From its 2011 Hack*, FORTUNE (Dec. 24, 2014), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[4] Seth Rosenblatt, *Modern Security Tactics Fail to Protect Against Malware, Study Finds*, CNET (Jan. 8, 2015), http://www.cnet.com/news/modern-security-tactics-fail-to-protect-against-malware-new-study-finds/.

[5] *Maginot Revisited* (2015), *supra* note 2; CYBERSECURITY'S MAGINOT LINE: A REAL-WORLD ASSESSMENT OF THE DEFENSE-IN-DEPTH MODEL, FIREEYE (2014), http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf. France created the Maginot Line during World War II to impede Nazi Germany's invasion, but German forces bypassed the Maginot Line and invaded France from Belgium. *See* MARC ROMANYCH ET AL., MAGINOT LINE 1940: BATTLES ON THE FRENCH FRONTIER 27 (2012).

[6] Sharon Tobias, *2014: The Year in Cyberattacks*, NEWSWEEK (Dec. 31, 2014), http://www.newsweek.com/2014-year-cyber-attacks-295876.

[7] *Maginot Revisited*, *supra* note 2, at 3.

passively wait for attacks. Instead, they should take a lean-forward approach that actively hunts for new and unseen threats."[8]

But what constitutes a lean-forward approach, and why are more organizations not already taking one? The emerging field of proactive cybersecurity is complex, encompassing a range of activities also referred to as "active defense." While "hacking back" is often a highly visible point of contention when discussing the role of private sector active defense,[9] it is just one facet of the larger proactive cybersecurity movement, which includes technological best practices ranging from real-time analytics to cybersecurity audits promoting built-in resilience.[10] Along with confusion about the range of activities that could be considered forward-leaning proactive cybersecurity, there remains ambiguity regarding the legality of some active defense techniques, including not only "hack back" but also "honeypots" and information sharing, two methods that have even been acknowledged by some governments as best practices for industry.[11]

This Article traces the evolution of the proactive cybersecurity industry in a global legal environment. We argue that, while hard law exists in this space both within the United States and globally, such laws were largely enacted at a time in which proactive cybersecurity remained nascent; as a result, the private sector has taken the lead in developing industry norms. More recently, we contend that proactive cybersecurity firms have thrived in part because of the confluence of three forces: (1) the general trend toward private security and growing awareness

[8] *Id*. at 21.

[9] *See, e.g.*, Carl Franzen, *Should US Companies Be Allowed to Hack China In Revenge? New Report Says Yes*, VERGE (May 22, 2013), http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back. *See also* Eric Chabrow, *The Case Against Hack-Back*, BANK INFO. SEC. (Jan. 6, 2015), http://www.bankinfosecurity.com/case-against-hack-back-a-7759; Tom Fields, *To 'Hack Back' or Not?*, BANK INFO. SEC. (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545 (discussing, among other things, the likelihood of prosecution in the United States for engaging in hacking back).

[10] *See, e.g.*, *Hackback? Claptrap!—An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for ("[a]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality"); *Proactive Cybersecurity – Taking Control Away from Attackers*, SYMANTEC (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cybersecurity/d/d-id/1108270.

[11] *See, e.g.*, Proactive Detection of Security Incidents II – Honeypots, European Union Agency for Network and Information Security (Nov. 20, 2012), https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots (which defines a "honeypot" as a "computing resource, whose sole task is to be probed, attacked, compromised, used or accessed in any other unauthorized way," at 17); Sean Lyngaas, *NIST Spells Out Information-Sharing Best Practices*, FCW (Oct. 30, 2014), http://fcw.com/articles/2014/10/30/nist-sharing-best-practices.aspx.

of cyber *in*security; (2) the unique nature of cybersecurity (with infrastructure that is often privately owned and for which private sector expertise dominates); and (3) the move toward bottom-up regulatory frameworks—in the vein of the 2014 National Institute for Standards and Technology ("NIST") Cybersecurity Framework, which aims to improve private sector cybersecurity through voluntary standards and was developed in coordination with industry.[12] Ultimately, we maintain that not only are these forces hastening the development and implementation of proactive cybersecurity measures, but that the law is hopelessly outdated and policy makers are lagging behind these developments—continuing to focus, for example, on the "hack back" question rather than on identifying, instilling, and spreading cybersecurity standards of behavior.

This Article thus seeks to situate and analyze the proactive cybersecurity movement through an analysis of industry practices and comparative regulations and is structured as follows. Part I contextualizes the emergence of active cyber defense, describing private sector attempts to use proactive technologies in the early 2000s as well as the reasons that such technologies did not achieve widespread adoption or attention at that point. We argue that the late 2000s and early 2010s represented a turning point because of the rise of progressively costly and sophisticated cyber attacks that gained increasingly widespread attention; for example, the attack against Google in 2010 and the company's responsive active defense actions in Operation Aurora helped to popularize the notion that companies themselves may need to engage cyber attackers to defend against Advanced Persistent Threats ("APTs").[13]

[12] *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, *available at* http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts; Update on the Cybersecurity Framework, NIST 4 (July 31, 2014), http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf ("NIST and other US government officials have had discussions about the Framework with multiple foreign governments and regional representatives including organizations throughout the world, including – but not limited to – the United Kingdom (UK), Japan, Korea, Estonia, Israel, Germany, and Australia."). For deeper background on the NIST Framework and how it relates to defining a standard of cybersecurity care, see Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, __ TEX. J. INT'L L. __ (forthcoming 2015).

[13] *See, e.g.*, Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14, 2010), http://www.wired.com/2010/01/operation-aurora/. This Article recognizes the possibility that—but does not consider whether—private firms more quietly used active cyber defense technologies before the early 2010s. Rather, it finds especially important and distinct the "open" or public adoption of such technologies because of the larger impact that such adoption will likely have on other private sector and governance trends.

Part I also provides an introduction to the global legal environment within which these proactive cybersecurity programs have been operating. Relatively little attention has been paid to the topic of proactive cybersecurity in the legal literature.[14] Articles that do focus on active cyber defense have done so predominantly within the international humanitarian law or U.S. context, neglecting comparative analysis that is vital to assessing applicable legal regimes, especially given the multinational presence of many of these firms as well as how easily cyber intrusions cross jurisdictions.[15] Our comparative analysis of the applicable law, anchored by comparisons to the U.S. legal environment, focuses primarily on the G8 nations; additional national approaches, including Singapore's unique law, are also considered.

Next, Part II assesses the post-2010, maturing proactive cybersecurity industry. It includes information from a survey of more than twenty cybersecurity firms, including Deloitte, IBM, and Lockheed Martin, demonstrating their range of proactive cybersecurity activities, as well as four in-depth case studies, highlighting the technologies and self-descriptive language recently launched proactive cybersecurity programs employ. In 2013, three boutique cybersecurity firms—including FireEye—and one government-associated nonprofit (in partnership with an investment firm) publicly launched proactive cybersecurity programs, resulting in a flurry of self-promotional materials and media attention. While separating themselves from illegal "hack back" techniques, the organizations underlined the necessity of

[14] *See, e.g.*, COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMM'N REP. 81 (2013).

[15] *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 1, 11 (2014) (discussing various active defense techniques); Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1259–63 (2014) (arguing for an amendment to the U.S. CFAA to include a limited self-help exception); Jay P. Kesan & Carol M. Hayes, *Mitigative Courterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415 (2012) (distinguishing between various active defense actions and definitions in the U.S. context but in reference to the applicable international law); Shane McGee, Randy V. Sabett, Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 5 (2013) (discussing the active defense debate in reference to the core issue of adequate attribution); Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 275 (2013) (arguing that existing international legal principles such as due diligence permit the use of private, proportionate cyber countermeasures); Melanie Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 227 (2013) (summarizing recent U.S. public and private cybersecurity developments); 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, 142 (2012) (arguing that private U.S. companies could be deputized under the CFAA); Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 319–20 (2013) (discussing the utility of various frameworks such as NERC in enhancing U.S. cybersecurity, but leaving out the NIST Cybersecurity Framework). *Cf.* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 104 (2014) ("[A]lmost certainly, hack back by a U.S. private sector actor will violate the domestic law of the country where a non-U.S. computer or server is located.").

proactive cybersecurity, citing the rise in APTs and the impossibility of effectively responding with only passive techniques.

Finally, Part III considers these organizations’ proactive cybersecurity programs by using the literature on “global security assemblages”[16] and polycentric governance[17] to demonstrate their likely staying power and implications for business practices and policymaking. In closing, we investigate the potential emergence of a proactive cybersecurity norm in international law along with the implications of this movement on contemporary Internet governance debates. While the private sector’s Internet governance role received two boosts in 2014—at NETmundial and the ITU Plenipotentiary Conference—challenges against it could be renewed if Western firms are perceived to push the norm-building process too aggressively, potentially undermining the multi-stakeholder model that the United States and others are attempting to sturdy[18] and impeding the promotion of “cyber peace.”[19]

[16] Rita Abrahamsen & Michael C. Williams, *Security Beyond the State: Global Security Assemblages in International Politics*, 3 INT’L POL. SOCIOLOGY 1, 1 (2009).

[17] This multi-level, multi-purpose, multi-functional, and multi-sectoral model, championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations “at multiple scales,” and examining the extent to which national and private control can in some cases coexist with communal management. Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL’Y STUD. J. 169, 171 (2011) (defining polycentricity as “a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes”); Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), *available at* http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

[18] *See, e.g.*, Grant Gross, *End of ICANN Contract Puts Internet Freedom at Risk, Critics Say*, PC WORLD (Apr. 10, 2014), http://www.pcworld.com/article/2142460/us-ntias-plan-to-end-icann-contract-puts-internet-freedom-at-risk-critics-say.html. Note that a comprehensive analysis of Internet governance and the U.S. position in this debate is beyond the scope of this paper. For useful background on these topics, *see, e.g.*, DAVID G. POST, IN SEARCH OF JEFFERSON’S MOOSE: NOTES ON THE STATE OF CYBERSPACE (2012); Milton Mueller and Ben Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, INTERNET GOVERNANCE PROJECT (2014), http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final_clean2.pdf.

[19] *See, e.g.*, Grant Gross, *End of ICANN Contract Puts Internet Freedom at Risk, Critics Say*, PC WORLD (Apr. 10, 2014), http://www.pcworld.com/article/2142460/us-ntias-plan-to-end-icann-contract-puts-internet-freedom-at-risk-critics-say.html. Note that a comprehensive analysis of Internet governance and the U.S. position in this debate is beyond the scope of this paper. For useful background on these topics, *see, e.g.*, DAVID G. POST, IN SEARCH OF JEFFERSON’S MOOSE: NOTES ON THE STATE OF CYBERSPACE (2012); Milton Mueller and Ben Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, INTERNET GOVERNANCE PROJECT (2014), http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final_clean2.pdf. For more on this topic generally, see preamble to SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

I. A SHORT HISTORY OF PROACTIVE CYBERSECURITY: CONCEPTS, IMPLEMENTATION, AND LEGALITY

Both the concepts and the jargon of "active defense" and "proactive cybersecurity" are rooted in military traditions.[20] For instance, not only ancient but also contemporary Chinese military generals have espoused the concepts in their most militaristic form,[21] and the U.S. military similarly adopted an active defense doctrine during the late twentieth century.[22] As in other warfare domains, cyberspace offers militaries opportunities to engage in proactive defense. For example, proactive defense may be operationalized through kinetic methods, like technologies that explode upon contact with antitank missiles, or through electronic measures, such as jamming an adversary's radar.[23] However, a review of the military's use of active cyber defense measures and the difficult issues related to determining when such measures may legally be used are beyond the scope of this Article.[24] Rather, here we focus on the use of active cyber defense measures by businesses because this term has "seeped into the private sector."[25]

This section first discusses the emergence of proactive cybersecurity as pursued by private sector organizations and individuals in the early to mid-2000s. Because pure defense has always been challenging in the realm of cybersecurity, some entities began to explore the utility of more proactive actions during this period, but technological, economic, and legal impediments

[20] *See, e.g.*, Keren Elazari, *Proactive Security: Integrating Active Defense in Cybersecurity*, GIGAOM RES. & CROWDSTRIKE (2013), at 7; McGee, Sabett, & Shah, *supra* note 15, at 2. It should be noted that the terms "active cyber defense" and "proactive cybersecurity" are often used interchangeably. However, active defense has a more narrow and military bent in some contexts leading to our preference for the term "proactive cybersecurity." *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 826 (2012) (defining "active defense" as including "electronic countermeasures designed to strike attacking computer systems and shut down cyber-attacks midstream.") (citing JEFFREY CARR, INSIDE CYBER WARFARE 46 (2010). Professor Dewar proposes more fine-grained definitions of active and passive defense based on proactive, fortified, and resilient defense mechanisms, because "Inconsistently applied terminology and concepts are further complicating an already complex issue." Robert S. Dewar, *The "Triptych of Cyber Security": A Classification of Active Defense,"* 6THANNUAL CONF. ON CYBER CONFLICT PROC. 7, 7 (2014).

[21] For instance, Sun Tzu famously said: "Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive." LIONEL GILES, ON THE ART OF WAR: THE OLDEST MILITARY TREATISE IN THE WORLD 99 (1910). Likewise, Mao Zedong famously said: "Only the active defense is the real defense." Wang Naiming, *Adhere to Active Defense and Modern People's War*, *in* CHINESE VIEWS OF FUTURE WARFARE 37, 38 (1998).

[22] *See, e.g.*, Jeffrey W. Long, The Evolution of U.S. Army Doctrine: From Active Defense to Airland Battle and Beyond (1991) (unpublished Masters thesis), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a241774.pdf.

[23] *See generally* Elazari, *supra* note 20.

[24] *See, e.g.*, Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent*, 201 MILITARY L. REV. 1 (2009); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87 (2010).

[25] *See generally* Elazari, *supra* note 20.

meant that such instances were relatively uncommon—or at least uncommonly publicized. To clearly demonstrate the legal impediments that may have forestalled the use of certain kinds of early proactive actions (including, most prominently, "hacking back"), this section then turns to legal regimes relevant to active defense. In addition to discussing relevant U.S. law, this section considers the laws of other G8 nations—with an in-depth look at the United Kingdom—and closes with a review of Singapore's recently updated and unique law. Finally, this section describes the emergence of APTs in the late 2000s, which likely encouraged more organizations to invest in cybersecurity and utilize more proactive technologies.

A. The Evolution of Active Cyber Defense

As cyber attacks have become progressively more troublesome and as governments and legal structures have oftentimes proven unhelpful to companies, the concept of active defense has increasingly entered the mainstream of private sector cybersecurity strategies.[26] The potential utility of proactive cybersecurity for the private sector started to gain traction in scholars' and companies' consciousness in the late 1990s and early 2000s. For instance, researchers began to explore the role of tools like honeypots, which are decoy servers or systems set up to gather information about intruders,[27] as supplements to traditional network security since at least 2003.[28] By 2005, more researchers were arguing that passive defense was inadequate in cyberspace because it allowed attackers' perceived risks to remain "nearly nil," creating a cost-benefit imbalance that significantly favored attackers.[29] Moreover, "[e]ven when passive defense technologies work correctly, they do not neutralize the costs incurred by an attack,"[30] meaning that firms often must double pay—for both the defensive technologies *and* for the costs of a successful attack. And as Robert Anderson, Brian Lum, and Bhavjit Walha have argued, the applicable U.S. "law provides little recourse" because it operates and adapts relatively slowly, is

[26] *See* Robert Anderson, Brian Lum, & Bhavjit Walha, *Offense vs. Defense* (White Paper, Dec. 11, 2005), http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefense.pdf.

[27] Loras R. Even, *Honey Pot Systems Explained*, SANS INST. (2000), http://www.sans.org/security-resources/idfaq/honeypot3.php.

[28] *See, e.g.*, FENG ZHANG ET AL., HONEYPOTS: A SUPPLEMENTED ACTIVE DEFENSE SYSTEM FOR NETWORK SECURITY, PARALLEL & DISTRIBUTED COMPUTING, APPLICATIONS, AND TECHNOLOGIES (2003).

[29] Anderson, Lum, & Walha, *supra* note 26, at 3.

[30] *Id.* at 2 (noting that "passive defense systems can do little more than drop malicious traffic," meaning that companies must still bear bandwidth, server usage, and wasted personnel costs. In addition, even if the attackers are somehow identified and apprehended, "there is still little hope of recovering the costs for the direct or indirect damages caused by the attack.").

jurisdictional, and requires the involvement of under-resourced enforcement agencies as is further discussed below.[31] These factors began to incentivize firms to seek a more effective "deterrent"—like proactive cybersecurity.[32]

Despite the potential benefits of such a deterrent, in the early and mid-2000s, open adoption of proactive cybersecurity technologies was limited; early examples include companies fighting piracy and companies (or individuals) trying to curtail the effects of spam or worms. For instance, the Motion Picture Association of America has a history of attempting to undermine online piracy by launching distributed denial of service ("DDoS") attacks, Trojan horses, and rootkits against movie pirates.[33] Similarly, in late 2004, Lycos Europe released a "Make Love not Spam" screensaver, which repeatedly requested data from known spammers.[34] The effort lasted less than one week, after which time Lycos Europe claimed that it was "too successful"—critics called it irresponsible and akin to a denial of service attack.[35] Meanwhile, Timothy Mullen, who is now the chief information officer and software architect for an accounting software firm, proposed shutting down the 2001 NIMDA worm by installing computer code that would alter the invaded host's boot sequence—conducting a "helpful intrusion."[36] Other examples abound. From 2003 to 2006, 419 Flash Mobs crashed fake bank sites, which facilitated 419 scams (i.e., advance-fee fraud).[37]

However, these efforts were relatively limited in scope and largely unorganized—and technological, economic, and legal limitations likely prevented the private sector's more widespread and methodic (as well as, perhaps, open) adoption of active cyber defense technology. First, though attribution remains a vexing issue today, in the mid 2000s, attribution represented an even more substantial technical hurdle.[38] In addition, most companies were likely

[31] *Id*. at 3, 12.

[32] *Id*. at 3, 7–10.

[33] *Id*. at 16. Though many cyber attackers have moved on from perceived less sophisticated DDoS attacks, their use is still prevalent. *See Hackers Anonymous 'Disable Extremist Website*,' BBC (Jan. 12, 2015), http://www.bbc.co.uk/newsbeat/30785773.

[34] Matt Hines, *Lycos Europe: 'Make Love Not Spam,'* CNET NEWS (Nov. 30, 2004), http://news.cnet.com/Lycos-Europe-Make-love-not-spam/2100-7349_3-5471207.html.

[35] Stuart Miles, *Lycos Makes Love Not Span Screensaver Taken Offline*, POCKET LINT (Dec. 5, 2004), http://www.pocket-lint.com/news/73865-lycos-make-love-not-spam-screensaver-taken-offline.

[36] Thomas C. Greene, *Attacking Nimda-Infected Attackers: Vigilance or Vigilantism?*, REGISTER (Aug. 8, 2002), http://www.theregister.co.uk/2002/08/08/attacking_nimdainfected_attackers/.

[37] *Flash Mob History*, ARTISTS AGAINST 419, http://wiki.aa419.org/index.php/Flash_Mob_History (last visited Sept. 17, 2014).

[38] Anderson, Lum, & Walha, *supra* note 26, at 5 (stating that the biggest technical hurdle "is that it is difficult to pin-point the exact source of [an] attack since source addresses can easily be spoofed); Keren Elazari, *supra* note 20, at 9

unwilling or unsure about how to invest significantly in IT security; according to Computer Security Institute surveys from 2003 to 2008, for example, most firms spent five percent or less of their IT budgets on security.[39] Cyber attacks were less prominent in the news and popular consciousness, meaning that private sector executives were less informed about them and less apt to encourage increased budgeting for IT security. Moreover, many companies adopted a reactive approach to cybersecurity, opting to respond to crises as they materialized due to the often-difficult cost-benefit analysis surrounding their efforts.[40] Finally, even technically advanced companies with expendable budgets may have shied away from proactive cybersecurity programs because of the uncertain legal status of "hacking back" in the United States.

B. Legal Uncertainty and the Computer Fraud and Abuse Act

The legal uncertainty shrouding elements of proactive cybersecurity arguably embodies the "biggest impediment to the deployment" of active cyber defense, especially with regard to the hack back debate.[41] From the start, researchers, IT professionals, and journalists have pondered whether so-called "Internet hack back" represents self-defense or vigilantism—a debate that persists today.[42] Even if they recognize such counter attacks as self-defense, researchers ask whether active defenders or non-malicious third parties, whose computers contribute to a botnet, should be held liable for any counter-attack damage.[43] Likewise, even if counterattacks are recognized as self-defense, additional legal issues may be raised if defenders access sensitive information—including financial, healthcare, or personally identifiable information—which is

(explaining that, as of 2013, attribution is a much more sophisticated endeavor; "[f]irst, you must know who the actor is; then you build that actor's profile, history, capabilities . . . .").

[39] *See* Robert Richardson, *Eight Annual Computer Crime and Security Survey*, COMP. SCI. INST. & FED. BUREAU OF INVESTIGATIONS (2003); Lawrence Gordon et al., *Ninth Annual Computer Crime and Security Survey*, COMP UTER SECURITY INSTITUTE AND FEDERAL BUREAU OF INVESTIGATIONS (2004), Lawrence Gordon et al., *10th Annual Computer Crime and Security Survey*, COMP. SCI. INST. & FED. BUREAU OF INVESTIGATIONS (2005); Lawrence A. Gordon et al., *CSI/FBI Computer Crime and Security Survey*, COMP. SCI. INST. & FED. BUREAU OF INVESTIGATIONS (2006); Robert Richardson, *CSI Computer Crime and Security Survey*, COMP. SCI. INST. (2007); Robert Richardson, *CSI Computer Crime & Security Survey*, COMP. SCI. INST. (2008).

[40] For more on this topic, see Scott Dynes, *Information Security Investment Case Study: The Manufacturing Sector*, CENTER FOR DIGITAL STRATEGIES (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/InfoSecManufacturing.pdf.

[41] Anderson, Lum, & Walha, *supra* note 26, at 5.

[42] *See, e.g.*, Vikas Jayawal, William Yurcik, & David Doss, *Internet Hack Back: Counter-Attacks as Self-Defense or Vigilantism*, IEEE INT'L SYMP. ON TECH. & SOC'Y (2002); Phil Harris, *Cyber Defense vs. Cyber Vigilante – Part 2 – Hacking Back*, SYMANTEC (July 16, 2013); Greene, *supra* note 36.

[43] Anderson, Lum, & Walha, *supra* note 26, at 14-15; Kenneth Einar Himma, *The Ethics of Tracing Hacker Attacks through the Machines of Innocent Persons*, 2 INT'L J. INFO. ETHICS 1, 1 (2004).

protected by other laws.[44] Likewise, how information is handled when collected in honeypots may be legally murky.[45] In addition, while threat information sharing is an acknowledged proactive best practice that many organizations utilize, such sharing may also sometimes be limited by legal ambiguities.[46] However, this section focuses primarily on laws that relate the unauthorized access of computers—such laws are not applicable to activities like information sharing but are legally controversial when applied to "hack back" activities.

The most relevant, if dated, applicable law in the U.S. context is the 1986 Computer Fraud and Abuse Act ("CFAA"). In particular, the CFAA, as amended in 2008, criminalizes "unauthorized access" to a computer or "unauthorized transmission" of things like malware (malicious software) as well as damaging a protected computer or network, obtaining and trafficking private information, and affecting the use of a computer (such as by using a computer to form a botnet).[47] Some argue that the broad strokes of the CFAA prohibit firms from infiltrating or otherwise manipulating attacking networks—even those located in foreign jurisdictions due to the law's extraterritorial reach; conversely, proactive cybersecurity measures that do not infiltrate other networks, such as honeypots used to gather information about and mislead cybercriminals, seemingly do not violate the CFAA.[48] What is often missed in the debate is that many nations now have similar laws in force—as we discuss below.[49]

Applying the CFAA to proactive cybersecurity is a complex undertaking, in part due to the schizophrenic approach of law enforcement. While law enforcement has discouraged a so-called "vigilante view," there is an unofficial understanding that "[law enforcement] can't handle the problem. It's too big. If you take care of things yourself, we will look in the other direction. Just be careful"—because problems still arise when companies "get caught or when innocent

[44] Irving Lachow, *Active Cyber Defense: A Framework for Policymakers*, CTR. NEW AM. SEC. 8 (Feb. 2013).

[45] *See* Jerome Radcliffe, *CyberLaw101: A Primer on US Laws Related to Honeypot Deployments*, SANS INST. 19 (2007).

[46] *See* David Inserra & Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Apr. 1, 2014), http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace (writing that some organizations would be more likely to share information if legal ambiguities in "outdated communications laws," the Wiretap and Stored Communication Acts, were resolved).

[47] *See* 18 U.S.C. § 1030; Jennifer Granick, *Amendments to Computer Crime Law Are a Dark Cloud with a Ray of Light*, EFF (June 15, 2009), http://www.eff.org/deeplinks/2009/06/amendments-computer. A botnet is a network of computers working together to perform some task, such as, in the best case, a citizen science project.

[48] *See* Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, CONG. RES. SERV., 6–7 (2010); Ellen Messmer, *Hitting Back at Cyberattackers: Experts Discuss Pros and Cons*, NETWORKWORLD (Nov. 1, 2012), http://www.networkworld.com/news/2012/110112-cyberattackers-263885.html.

[49] Anderson, Lum, & Walha, *supra* note 26, at 13, 15.

bystanders are harmed."[50] But if alleged victims of a counterattack are less sympathetic, then courts may also favorably interpret active defense actions. For example, in 2000, Ehippies, a U.K.-based online activist group, hit Conxion—a San Jose, California hosting service—with a denial of service attack, and rather than dropping the incoming packets, Conxion "volleyed them back" at the activist group's server, shutting it down for several hours.[51] Conxion's actions—defined as "returning mail to sender"—were subsequently deemed legal.[52]

Moreover, Stewart Baker, former assistant secretary for policy at the U.S. Department of Homeland Security (DHS), has argued that defenders who retrieve their stolen data may not violate the CFAA by accessing—without "authorization"—an attacker's computer because defenders *are* authorized by their ownership of illegally seized data, such as trade secrets, on that attacker's computer.[53] However, Professor Orin Kerr has responded that the CFAA protects the rights of computer owners rather than data owners, so Baker cannot circumvent authorization requirements by asserting defenders' rights to their own data. These and other debates surrounding the applicability of the CFAA to hacking back—which is just one potential method in a proactive cybersecurity program—are largely unresolved in the United States.

C. A Comparative Analysis of Proactive Cybersecurity Regulation

In an effort to place the topic of proactive cybersecurity regulation in greater global context, we next compare the CFAA with national analogues from other G8 nations, which, along with the United States, are: Canada, France, Germany, Italy, Japan, Russia, and the United Kingdom (UK). These countries were selected because they are among the most advanced and sophisticated cyber powers, and even though the existence of the G8 as a forum has been severely tested by Russia's actions in Crimea and elsewhere, Russia's cyber stature motivated us to include its laws in our analysis. In this section, we also look further afield at other nations with active defense regulations on the books to ascertain whether norms might be emerging in

[50] *Id*. at 22.

[51] Deborah Radcliff, *Should You Strike Back?*, COMPUTER WORLD (Nov. 13, 2000), http://www.computerworld.com/s/article/53869/_Should_You_Strike_Back_?pageNumber=2.

[52] *Id*. ("Chris Malinowski, the recently retired lieutenant commander of the New York Police Department's Computer Crime Squad, says 'returning mail to sender' doesn't constitute a crime. But many information technology professionals say they wouldn't risk taking such an action, even if they had explicit proof of the source of the attack. The chief concern is accidentally slamming innocent sites through which hackers have routed their attacks to conceal their tracks.").

[53] Stewart Baker, Orin Kerr, & Eugene Volokh, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

the proactive cybersecurity space—with important implications for businesses and policymakers. First, though, we turn to an in-depth case study of the UK's laws related to active defense, beginning to define the regulatory spectrum at work in the field of proactive cybersecurity.

1. In-Depth Comparative Case Study: Comparing the U.S. and UK Experiences with Proactive Cybersecurity

The development of the UK Computer Misuse Act ("CMA") in many ways mirrors the development of the CFAA. Both were enacted before the World Wide Web (1984 and 1990); both regulate the concept of "unauthorized access"; and both provide expansive protection to covered computer systems. Yet differences between these laws are also apparent. While the CFAA relies upon broad definitions of "protected computer" to effectively cover any computer system connected to a network,[54] the CMA provides no explicit definition of "computer," "program," or "data," allowing this definitional ambiguity to be resolved by the courts.[55] In many ways, these were prescient omissions, as the British Parliament recognized that technological advancements could render the initial definitions obsolete, highlighting the need for rapid, organic evolution through the judicial process.[56] This definitional laxity has also enabled the CMA's statutory substance to remain relatively unchanged in the 20 years since its enactment, with the only substantive amendment being the Police and Justice Act of 2006.[57]

Despite the CMA's comparatively sparse text, it has been interpreted to be effectively as expansive as the CFAA. The CMA relies upon the concept of "authorisation" to do most of its interpretive work, as can be seen in the case of *Regina v. Bow Street Magistrates Court and Allison*, which effectively tested the CMA's application to the concept of "exceeds authorized access" under the CFAA.[58] *Allison* involved a conspiracy in which an employee at American Express used her network access to steal account information from customers not assigned to her; then, her co-conspirator withdrew large sums of money from those accounts. The magistrate

[54] *See* Orrin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN L. REV. 1561, 1577–78 (2010) (citing 18 U.S.C.A. §1030(e) (observing that "protected computer" under the CFAA covers nearly all computers).

[55] *See* All Party Parliamentary Internet Group, "*Revision of the Computer Misuse Act": Report of an Inquiry by the All Party Internet Group*, APIG, http://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf (last visited Nov. 12, 2014).

[56] *Id*. at 4.

[57] Stefan Fafinski, *The UK Legislative Position on Cybercrime: A 20 Year Retrospective*, 13 J. INTERNET L. 3, 10 (2009).

[58] *R.v. Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America*, House of Lords, [1999] UKHL 31 (Eng.).

found that the CMA did not cover the act, as the "access" in question was authorized due to the perpetrator's status as an employee of the company. However, on appeal (also pursued by the U.S. government, seeking extradition), the House of Lords held that the magistrate misunderstood the concept of authorization.[59] The issue was not authorization to the network but authorization to the specific data in question, which this defendant did not have.[60] This effectively expanded the offense of unauthorized access to encompass the concept of "exceeds authorized access," demonstrating the practical similarity between the CMA and the CFAA.

Despite the broad interpretive prerogative given to the UK courts, certain areas still occupy a legal gray zone, including active defense. The most-discussed area of legal uncertainty in the British context is the use of denial of service ("DoS"), DDoS, and other cyber attacks that repeatedly engage in "unauthorized" activity to harass or impair. This issue was addressed directly in the case of *Director of Public Prosecutions v. Lennon*, wherein a disgruntled former employee used a mailbox spammer to overload a former employer's email server, disrupting its operability.[61] As in *Allison*, the magistrate found that the CMA did not cover the act, as an email server implicitly authorizes the receipt of email. However, the Divisional Court rejected this logic, relying instead on a more holistic analysis that queried not whether each individual email was authorized but whether the transaction as a whole was authorized.[62] Under this view, the Court held that the email server did not authorize the bulk receipt of junk email.[63] (It was careful, however, to distinguish intentional attacks from incidental spam email.) Yet despite this clarification with regard to email spammers, and an abundance of cases convicting defendants of DDoS and DoS attacks, there are still calls for legislation specifically addressing the issue.[64]

The issue of active defense generally, although less discussed than DDoS and DoS attacks, has not been ignored in the UK. In the 2004 Inquiry into the Revision of the Computer Misuse Act by the All Party Internet Group ("APIG"), the British Parliament raised concerns over the legality of "active measures" to ensure its server security.[65] The APIG interpreted "active measures" as the proactive scanning of customers to identify potential security holes,

[59] *Id.*
[60] *Id.*
[61] *DPP v. Lennon*, (Wimbledon magistrate's Court, 2 Nov. 2005) (Eng.).
[62] *DPP v. Lennon*, [2006] EWHC 1201 (Admin) (Eng.).
[63] *Id.*
[64] *Id.*
[65] APIG, *supra* note 55, at 8.

which is only a subset of how we define proactive cybersecurity in this Article.[66] Although the group recognized the potential legal ambiguity in terminology, it decided against enacting specific legislation, arguing that these issues were better resolved through contract.[67] In its view, the British Parliament should explicitly contract that its "active measures" were authorized, thereby not falling under the ambit of the CMA. The APIG worried that any legislation broadly allowing such scanning might facilitate excessive and unwarranted intrusions by companies of their customers, a situation that it wished to avoid.[68] This case once again highlights the significance of the concept of authorization under the CMA and of the parliamentary reluctance to enact further cybersecurity legislation where other regulatory modalities may be preferable. Yet it must be noted that the "active measures" they discussed did not explicitly extend to criminal activities, a situation in which contract would logically not be a workable solution.

Although the APIG's deferral to contract might suggest leniency in the area of active defense, the UK courts have historically taken a fairly hard line against preventative measures in the absence of explicit authorization. In the case of *Regina v. Cuthbert*, the defendant was skeptical of a website's authenticity and tested it to ensure that it was not fraudulent.[69] He was attempting to donate to disaster relief for the 2004 tsunami but felt that the website looked illegitimate, so he performed minimally invasive (yet unauthorized) tests to ensure its veracity. When brought to trial, the defendant admitted to these "minimal breaches" and argued that he could have engaged in much more invasive activities had he wanted to. Despite the good faith nature of his actions and their minimal scope, the magistrate convicted him.[70]

As is highlight in *Regina v. Cuthbert*, in addition to the definitional differences between the CMA and CFAA, the UK system of relief is also unlike the U.S. model in that it allows for private prosecutions as an additional remedy for aggrieved parties.[71] Such private prosecutions have long been a part of the UK legal system, with widespread public prosecution being a comparatively recent phenomenon.[72] The APIG specifically addressed providing prosecutorial discretion to private parties as a potential remedy to insufficient law enforcement resources and an abundance of cases, resolving to recommend that the Director of Public Prosecutions set out a

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *R. v. Cuthbert,* [2005] EWHC (Admin) (Eng.).
[70] *Id.*
[71] APIG, *supra* note 55, at 16
[72] *Id.*

permissive policy for private prosecutions under the CMA.[73] Yet this option of private prosecution would not extend the enhanced investigatory powers enjoyed by the state and, as such, would not allow for active defense activities that would not otherwise be legal under the CMA. (Also, rather ironically, the APIG declined to suggest allowing private prosecutions by individuals in small claims courts, citing the difficulties of attribution discussed above.[74])

Other differences between the CMA and CFAA are illustrated by the debate between Baker and Kerr introduced above, including the assertion that the CMA is arguably data protective rather than computer protective, meaning it may be more amenable to active defense than the CFAA.[75] Since the CMA arguably places a greater emphasis on the authorization to access data, Baker's analogies with traditional tort and criminal law are more appropriate. Arguably, engaging in active defense (or perhaps even more aggressive hack back activities) when retaking data (as its true owner) is implicitly authorized when criminals steal or subvert a company's data.[76] The CMA also differs from the CFAA in its heightened reliance on mitigating and aggravating factors to determine sentencing. Although both acts consider these factors, the CMA places a greater emphasis on the culpability of the victim (in this case, the party subject to "active defense"), the sophistication of the attack, and the existence of any provocation for the attack.[77] British courts may therefore view active defense more favorably than some U.S. courts, as any unauthorized access that may occur from a firm's proactive cybersecurity practices would be considered in light of the unauthorized access that it suffered.

Ultimately, though, the UK's CMA is burdened by the same problem as the CFAA: these statutes were not drafted to regulate the field of proactive cybersecurity. Although both acts have proven somewhat adaptable to the rapidly changing technological environment and have been amended in the mid-2000s, they are both nonetheless outdated and would need to be further updated to address more nuanced concerns that advancing technology, multiplying actors, and evolving geopolitics have created. To broaden our context, and consider some similarly situated countries with more recently adopted criminal access laws, we next turn to the remaining six nations of the G8. Without evaluating each country's law uniquely, we engage in a comparative analysis; relevant language from each statute is included in Table 1 below.

[73] *Id.*

[74] *Id.* at 17.

[75] *See infra* note 53 and associated text.

[76] *Id.*

[77] *Id.*

2. Regulating “Unauthorized Access” Across the G8

Many nations around the world are grappling with the policy questions that are vexing U.S. and UK firms and regulators, and understanding this regulatory complexity is vital, even for U.S.-based firms. After all, cyber attacks impact the operations of multinational enterprises every day and oftentimes pass through myriad jurisdictions on their way to and from targeted systems, opening the door for confusing conflict of laws scenarios to play out.[78] It is beyond the scope of this Article to provide a full accounting of global cyber active defense regulation, though that would be a helpful research project for scholars to pursue. Rather, we focus here on the applicable laws and regulations of the G8 Member States relating to the active defense debate, summarized in Table 1, to help introduce this regulatory complexity and better inform both businesses and policymakers of the legal obstacles and opportunities present in this space.

TABLE 1: SAMPLE OF REGULATIONS FROM G8 NATIONS PERTAINING TO PROACTIVE CYBERSECURITY[79]

COUNTRY	TITLE OF LAW	YEAR OF LAW	RELEVANT LANGUAGE

[78] *See, e.g.*, *The Attribution Problem in Cyber Attacks*, INFOSEC INST., http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/ (last visited Nov. 8, 2014); Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/.

[79] These data were assembled from the following sources: L*aws of Canada as they Pertain to Computer Crime*, SANS INST. INFOSEC RDG. RM. (2001), http://www.sans.org/reading-room/whitepapers/legal/laws-canada-pertain-computer-crime-673; Cybercrime and the *Criminal Code*, CAN. DEP’T OF JUSTICE (2012), http://www.oas.org/cyber/presentations/Norm%20Wong%20-%20OAS%20Cybercrime.pdf; CyberCrime Law, http://www.cybercrimelaw.net/France.html (last visited Nov. 23, 2014); Valéry Marchive, *Cyberdefence to Become Cyber-Attack as France Gets Ready to go on the Offensive*, ZDNET (May 3, 2013), http://www.zdnet.com/cyberdefence-to-become-cyber-attack-as-france-gets-ready-to-go-on-the-offensive-7000014878/; CyberCrime Law, http://www.cybercrimelaw.net/Germany.html (last visited Nov. 23, 2014); Bettina Weisser, *Cyber Crime – The Information Society and Related Crimes* (2013), http://www.penal.org/spip/IMG/file/RM-8.pdf; CyberCrime Law, http://www.cybercrimelaw.net/Italy.html (last visited Nov. 23, 2014); CyberCrime Law, http://www.cybercrimelaw.net/Japan.html (last visited Nov. 23, 2014); Graeme McMillan, *Japan Criminalizes Cybercrime: Make a Virus, Get Three Years in Jail*, TIME (June 17, 2011), http://techland.time.com/2011/06/17/japan-criminalizes-cybercrime-make-a-virus-get-three-years-in-jail/; Japanese Cyber Security Strategy and related Documents, http://www.space-cyber.jp/cyber/ (last visited Nov. 23, 2014); Ryusuke Masuoka & Tsutomu Ishino, *Cyber Security in Japan*, CIPPS (2012), http://www.cipps.org/group/cyber_memo/003_121204.pdf; Takato Natsui, *Cybercrimes in Japan: Recent Cases, Legislations, Problems and Perspectives*, http://www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf; Robert Lipovsky, Aleksandr Matrosov, & Dmitry Volkov, *Cybercrime in Russia: Trends and Issues*, ESET (2011), http://www.eset.com/us/resources/white-papers/CARO_2011.pdf; David Emm, *Cybercrime and the Law: A Review of UK Computer Crime Legislation*, Sec. List (May 29, 2009), http://securelist.com/analysis/publications/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/; CyberCrime Law, http://www.cybercrimelaw.net/UK.html (last visited Nov. 23, 2014).

Canada	• Criminal Code of Canada § 342.1 • Criminal Code of Canada § 430(1.1)	• 1985 • 1985	• “Everyone who fraudulently, and without colour of right, obtains, directly or indirectly, any computer service … is guilty of an indictable offense …” • “Every one commits mischief who willfully a. Destroys or alters data; b. Renders data meaningless, useless, or ineffective; c. Obstructs, interrupts, or interferes with the lawful use of data; or d. Obstructs, interrupts, or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto
France	Penal Code Article 323-1	2000 (not in force until 2002)	“Fraudulent accessing or remaining within all or part of an automated data processing system is punished by a sentence not exceeding two years’ imprisonment and a fine of 30.000 euro”
Germany	Penal Code Section 202(a): Data Espionage	1998	“Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine.”
Italy	Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems	2008	“Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.”
Japan	Law No. 128, Article 3: Unauthorized Computer Access Law	1999 (In effect in 2000)	“No person shall conduct an act of unauthorized computer access . . . .”
Russia	Penal Code Chapter 28, Article 272: Illegal Accessing of Computer Information	1996	“Illegal accessing of legally-protected computer information … shall be punishable by a fine in the amount of 200 to 500 minimum wages, or in the amount of the wage or salary, or any other income of the convicted person for a period of two to five months, or by corrective labour for a term of six to twelve months, or by deprivation of liberty for a term of up to two years.”
United Kingdom	Computer Misuse Act	1990 (amended in 2006—Police and Justice Act, Section 35)	“(1)A person is guilty of an offence if— a. he causes a computer to perform any function with intent to secure access to any program or data held in any computer [or to enable any such access to be secured] b. the access he intends to secure [or to enable to be secured,] is unauthorised; and c. he knows at the time when he causes the computer to perform the function that that is the case.”

United States	• USA Patriot Act • Computer Fraud and Abuse Act	• 18 U.S.C. § 1030 (2001) • 8 U.S.C. § 1030 (1984, last updated 2008)	• This Amendment to the Patriot Act pertains to “computers outside of the United States so long as they affect ‘interstate or foreign commerce or communication of the United States.’[80] • The Computer Fraud and Abuse Act regulates those who “knowingly” or “intentionally” access “a computer without authorization or exceeds authorized access . . . .” 18 U.S.C. § 1030(a)(2). • The Department of Justice has noted that “[t]he term ‘without authorization’ is not defined by the CFAA. The term ‘exceeds authorized access’ means ‘to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.’ 18 U.S.C. § 1030(e)(6).”[81]

The first important commonality to note is that every G8 nation has a law on the books that regulates “unauthorized access” to a greater or lesser extent. Such laws are primarily focused on criminalizing hacking (rather than “hacking back”), and such commonality may be due to the influence of the Council of Europe Convention on Cybercrime (“Budapest Convention”), but in any case, such congruence is important to note.[82] For example, Canada passed the relevant provisions of its Criminal Code in 1985 shortly after the CFAA was introduced in the U.S. Congress. Other G8 members—including Germany, Russia, and the UK—passed relevant laws in the 1990s, while the remainder—including France, Italy, and Japan—did not regulate this behavior until the 2000s. No G8-created, active defense-related law that we could locate, including amendments to existing legislation such as the CFAA or Italy’s Penal Code, has been passed or amended since 2008—a gap of time in which, as the below section describes, cybercrime practices have evolved a great deal.[83]

[80] For a thorough review of U.S. cybercrime law as it pertains to active defense and “hacking back,” see Dep’t of Justice, Prosecuting Computer Crimes (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[81] *Id*. at 5.

[82] Although the Budapest Convention itself is silent on the matter, Professor Paul Rosenzweig has noted that a 2001 Explanatory Report includes language to the effect that “the Parties are free, if they wish, to permit such [active defense] conduct when it occurs pursuant to established legal defenses, excuses, or justification.” Rosenzweig, *supra* note 15, at 109 (citing Counsel of Europe, Explanatory Report to the Convention on Cybercrime, E.T.S. No. 185 (Nov. 23, 2001), *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

[83] *See, e.g.*, Cybercrime: An Evolving Risk to Business, EY (2013), http://www.ey.com/Publication/vwLUAssets/ey-cybercrime-an-evolving-risk-to-businesses/$FILE/ey-cybercrime-an-evolving-risk-to-businesses.pdf.

Other areas of convergence across the G8 also exist. Each surveyed nation references the imposition of fines and jail time, though the quantity of each varies greatly. In France, for example, hacking can result in a 30,000 euro fine, while in Russia an alleged criminal could face the loss of up to "500 minimum wages . . . ."[84] The length of potential jail time, though, does show more consistency, with two-to-three year sentences common in France, Germany, Italy, Russia, and the United States (though, in the latter, sentences can run up to 20 years depending on the type of breach under the CFAA).[85] Many of the laws are also written quite broadly, with the United States and UK pursuing similar approaches of regulating unauthorized access as was discussed above, including levying an explicit intentional (rather than "knowing") mental state requirement.[86] Even more broadly, Canada's Criminal Code regulates unauthorized access broadly as "[e]veryone [who] commits mischief."[87]

An area of divergence among the G8 is the degree of protection required for a breach to occur. In Germany, for example, a person who obtains data without authorization from a system "specially protected against unauthorized access" is deemed to have broken the law.[88] Similarly, in Italy, only those computers that are "protected by security measures" are covered by the Penal Code.[89] Prosecutors in Germany and Italy could, for example, then have to argue about whether the system that a defendant is accused of breaching was secure or otherwise specially protected. In contrast, Canada, France, Japan, the UK, and the United States are broader in their application of unauthorized access laws in that they have no specific provision on required security or protection for the breached computer system or data.

Political divergence may also be occurring. As a group, the G8 has worked to fight global cybercrime since at least 2006.[90] In 2007, the G8 agreed "to work towards criminalizing, within national legal frameworks, specific forms of misusing the Internet for terrorist purposes."[91] Then, in 2010, G8 members agreed on declarations referencing the need to take action to "weaken the ability . . . of transnational organized crime groups to operate."[92]

[84] Penal Code Art. 323-1 (F4.); Penal Code Chapter 28, Art. 272: Illegal Accessing of Computer Information (Rus.).
[85] *See* PROSECUTING COMPUTER CRIMES, *supra* note 80, at 3 tbl. 1.
[86] *Id*. at 17.
[87] Criminal Code of Canada § 430(1.1) (Can.).
[88] Penal Code Section 202(a): Data Espionage (Ger.). *See also* Rosenzweig, *supra* note 15, at 114.
[89] Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems (Italy).
[90] *See Cybercrime Law*, G8, http://www.cybercrimelaw.net/G8.html (last visited Nov. 8, 2014).
[91] *Id*.
[92] G8 Muskoka Declaration, para. 42 (June 25-26, 2010), http://www.mofa.go.jp/policy/economy/summit/2010/pdfs/declaration_1006.pdf.

However, Russia's actions in Crimea and elsewhere in 2014 have led to far less emphasis on the G8 as a vehicle to harmonize national approaches to cybersecurity, resulting in greater emphasis on the G20.[93] There have also been calls for the G20 to deepen partnerships with multinational tech firms to better combat cybercrime, a "G20 plus 20" strategy.[94] Moreover, as cybercrime and private sector strategies are global issues in an increasingly multipolar world,[95] looking beyond the G8 is especially important. As such, the next section looks beyond how the United States, UK, and other similarly situated nations to consider Singapore's and others' approaches.

3. Understanding Singapore's New Approach

Singapore, a major world financial center, has been the victim of a series of relatively high profile attacks and breaches in recent years, and its 2014 amendment to its Computer Misuse Act (retitled the Computer Misuse and Cybersecurity Act ("CMCA"))[96] is part of an attempt to address the country's systemic shortage of cybersecurity professionals.[97] The amendment marked the beginning of its second Infocomm Security Masterplan, a period of cybersecurity development extending to 2018 (the first Infocomm Security Masterplan spanned 2005-2007).[98] Both plans are multifaceted national strategies to promote cybersecurity at a systemic level and reflect Singapore's need for broader cybersecurity reform. Given Singapore's profile as a high-value target with relatively poor private sector cybersecurity,[99] it has decided to pursue more aggressive national cybersecurity policy than many Western nations in the form of the CMCA.

The CMCA is significant in that it crafts a middle ground in the realm of active defense policymaking: whereas it does not fully legalize private active defense, it does create a mechanism for state-sanctioned active defense to protect critical national infrastructure. The

[93] *See* Thalif Deen, *Russia Expelled from G8, but G20? Not So Fast*, IPS PRESS SERV. (Apr. 1, 2014), http://www.ipsnews.net/2014/04/russia-expelled-g8-g20-fast/.
[94] Raymond Hainey, *Beefing Up Cyber Crime Fight*, ROYAL GAZETTE (Oct. 7, 2014), http://www.royalgazette.com/article/20141007/BUSINESS/141009813.
[95] *See, e.g..*, *Insight Report – Global Risks 2014: Ninth Edition*, WORLD ECONOMIC FORUM (2014), http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, at 10.
[96] Computer Misuse and Cybersecurity Act (Cap. 50A, 2013 Rev. Ed) (Sing.).
[97] Leonal, Brian. *Cybersecurity Skills Shortage Poses Threat in Singapore.* BLOOMBERG, Jun 22, 2014, http://www.bloomberg.com/news/2014-06-22/cybersecurity-skills-shortage-looms-in-singapore-southeast-asia.html
[98] *Infocomm Security Masterplan 2*, INFOCOMM DEV. AUTHORITY OF SINGAPORE, http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/Infocomm-Security-Masterplan-2 (last visited Nov. 12, 2014).
[99] Ellyne Phneah, *Global politics hinder Singapore as 'Switzerland of cybersecurity,'* ZDNet (June 27, 2013), http://www.zdnet.com/article/global-politics-hinder-singapore-as-switzerland-of-cybersecurity/ (explaining that there is a "lack of a talent pool" because "local universities currently do not have many specialized programs or divisions" to "provide opportunities for people to learn more about cybersecurity").

amendment permits the governmental issuance of certificates directing "specified persons" (individuals or organizations) to prevent, detect, or counter specific threats to critical infrastructure, including the power to criminalize non-compliance, while providing prosecutorial immunity to the specified persons.[100] Effectively, the amendment allows the Minister to imbue private parties with the powers typically enjoyed by the state—so that they may more effectively combat the multifaceted cyber threat faced by critical infrastructure operators.[101] Moreover, according to a statement by the Ministry of Home Affairs, the Minister may empower the specified person to take preemptive strikes against perceived cyber threats, representing arguably the most aggressive interpretation of private active defense codified by a nation-state to date.[102]

Singapore's strategy marks an interesting development in the active defense debate. With regard to more aggressive active defense activities like "hack back," the primary concerns have long been that private actors' use of these technologies could escalate cyber conflicts or be directed against the wrong entities, especially given the technical and legal difficulties surrounding attribution.[103] By requiring state authorization, Singapore is able to enjoy the benefits of using private actors as primary responders to cyber threats while taking some measures to maintain accountability and limit the extent to which the private "persons" may act. Ultimately, the efficacy of the law will in part depend on the speed at which the government can respond to requests for this heightened power; an overly bureaucratic system may simply be too slow to allow for a meaningful response. Moreover, allowing for state-sanctioned cyber responses does not clarify the requirements for attribution before action, which private entities will be certified, or the legality of other proactive cybersecurity discussed in Part II.

Beyond Singapore, myriad other nations, ranging from Albania to Fiji and Jamaica, have passed similar laws that are applicable to active cyber defense. A sampling of such laws is included in Appendix A. For example, in Dominica, "A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system" is guilty of violating the penal code,[104] whereas a 2009 Kenyan law states: "Any person who causes a computer system to perform a function, knowing that the access he has secured is unauthorized,

[100] CMCA, *supra* note 96, at Part III, § 15A(1).
[101] *Id.*
[102] Phneah, Ellyne, *S'pore Beefs up Cybersecurity Law to Allow Preemptive Measures,* ZDNET (Jan. 14, 2013), http://www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/.
[103] *See, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 58 (2013) (noting some of the difficulties involved with attributing a cyber attack back to a particular individual).
[104] Dominican Penal Code, Part II, § 5 (Dominica).

shall commit an offence."[105] This brief survey suggests that, rather than being the exclusive purview of the most developed or wired nations in the world, the field of cybercrime—with resulting impact on "hacking back," a subset of proactive cybersecurity—is increasingly an arena of interest to policymakers the world over. Excepting Singapore, though, few if any nations are keeping up with the rapid evolution of the proactive cybersecurity industry and addressing active defense in regulation. Instead, as this legal survey has demonstrated, much of the regulatory emphasis has been on shaping the legal environment for "unauthorized access."

However, the actions, policies, and techniques of the proactive cybersecurity industry are much more dynamic—as Section II demonstrates. While policymakers, quite rightly, rarely get into the minutia of defining cybersecurity best practices,[106] more officials are paying attention to cybersecurity. In the European Union, for instance, the 2013 cybersecurity strategy encourages nations to establish cybersecurity performance standards and limit turf battles between agencies; at the regional level, the strategy clarifies the roles of CERT-EU, the European Network and Information Security Agency, and the European Cybercrime Center, among other agencies, to respond to different categories of cyber attacks up to a major incident.[107] Moreover, it suggests establishing "appropriate cybersecurity performance requirements" and mandatory reporting for cyber attacks having a "significant impact" on firms operating across a broad array of sectors.[108] These developments could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates . . . ."[109] In some ways, then, this regime could

[105] Information and Communications Act, Part VIA 83U (Kenya).

[106] Examples of best practices include the use of regular penetration testing, cybersecurity analytics, and auditing.

[107] *See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 4–5, 17–19 (Feb. 7, 2013) [hereinafter *EU Cybersecurity Strategy*] (the proposal includes five strategic priorities: (1) to "achiev[e] cyber resilience"; (2) to "[d]rastically reduc[e] cybercrime; (3) to "develop[] [a new] cyberdefense policy"; (4) to "[d]evelop the industrial and technological resources for cybersecurity"; and (5) to "[e]stablish a coherent international cyberspace policy for the European Union and promote core EU values.").

[108] *Id.* at 2, 12.

[109] Warwick Ashford, *How Will EU Cyber* Security *Directive Affect Business?*, COMPUTER WKLY (Feb. 19, 2013), http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive-affect-business (citing Stewart Room, a partner at Field Fisher Waterhouse, who argues that this directive will mean that other firms beyond telecom companies will face regulatory burdens related to cybersecurity. These will include "e-commerce platforms; [I]nternet payment gateways; social networks; search engines; cloud computing services; app stores."). Among much else, companies with some nexus to the Internet would need to invest in new technologies, develop procedures to prove compliance to national and E.U. regulators, and undertake enhanced cyber risk mitigation measures to better manage attacks. *Id.* at 2–6. *But see* Stephen Gardner, *Member States Reportedly Unconvinced on Need for EU Cybersecurity Directive*, BLOOMBERG BNA (June 3, 2013), http://www.bna.com/member-states-reportedly-n17179874317/ (reporting on questions from ministers arising from this mandate approach and noting that "other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard

codify and regionalize aspects of the proactive cybersecurity movement that are less controversial than hacking back, aiding in international norm development, which is further discussed in Part III. First, thought, this section returns to the narrative with which it began, jumping to the end of the 2000s and the emergence of APTs, which prompted some companies to expand research and utilization of a broader array of proactive cybersecurity technologies.

D. The Private Sector Pushes Forward: A New Era in Proactive Cybersecurity

In the late 2000s and early 2010s, despite continued legal uncertainty in the United States and globally, debates about active cyber defense began to shift. More frequent cyber attacks[110] and companies' increasing anxiety likely contributed to this change of perception; for instance, by 2010, more than 40 percent of companies surveyed by Symantec reported that cybersecurity incidents topped their lists of concerns.[111] As was mentioned above, one watershed moment was Operation Aurora, a sophisticated campaign using spear phishing attacks and at least one zero-day exploit exposed by Google in early 2010.[112]

The attacks were noteworthy for at least two reasons: the type of intellectual property that was stolen (including Google's source code—that is, its "crown jewels"[113]); and the illustration of the extent to which state-sponsored attacks—or other highly organized and well-financed attackers—had begun targeting private firms.[114] According to Dmitri Alperovitch, then-vice president of threat research at the anti-virus firm McAfee, Operation Aurora "totally" changed

to cybersecurity standards" such as the NIST Cybersecurity Framework and worrying about creating "inconsistencies for companies whose operations span several jurisdictions . . . .").

[110] *See, e.g.*, John Markoff, *Thieves Winning Online War, Maybe Even in Your Computer*, N.Y. TIMES (Dec. 5, 2008), http://www.nytimes.com/2008/12/06/technology/internet/06security.html?scp=1&sq= +internet%20crime%20bad%20guys&st=cse; Kevin Voigt, *Cyber Crime Poses Threat to E-commerce*, CNN (Dec. 14, 2009), http://www.cnn.com/2009/TECH/12/13/cybercrime.2009.review/index.html?iref=allsearch.

[111] *State of Enterprise Security Study*, SYMANTEC (2010), http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01.

[112] *See* Michael J. Gross, *Enter the Cyber-dragon*, VANITY FAIR (Sept. 2011), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109; Brian Grow & Mark Hosenball, *Special Report: In Cyberspy vs. Cyberspy, China Has the Edge*, REUTERS (Apr. 14, 2011), http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414; Kim Zetter, '*Google' Hackers Had Ability to Alter Source Code,* WIRED (Mar. 3, 2010), http://www.wired.com/threatlevel/2010/03/source-code-hacks/.

[113] Zetter, *supra* note 112.

[114] *See Report to Congress*, U.S.-CHINA ECON. & SEC. REV. COMMISSION 168 (U.S. Naval Inst., 2012) (reporting that "[i]n 2012, Chinese state-sponsored actors continued to exploit government, military, indsutrial, and nongovernmental computer systems."); VERIZON, DATA BREACH INVESTIGATIONS REPORT 5, 21–22 (2013), http://www.verizonenterprise.com/DBIR/2013/ [hereinafter DBIR 2013] (reporting that state-sponsored attacks accounted for 19 percent of all reported attacks, with organized crime being the biggest external source at 55 percent).

the threat model, representing the first instance in which private firms (outside defense contractors) experienced "that level of sophisticated attack."[115] Moreover, in Google's private investigation, the company gained access to a computer, located in Taiwan, "that it suspected of being the source of the [Aurora] attacks."[116] When it saw evidence of attacks involving other U.S. companies, Google alerted and collaborated with U.S. intelligence and law enforcement agencies to trace ultimate responsibility for the attacks back to mainland China.[117] As such, Google may have "set a precedent of what is allowable" to defend against APTs—even as "one could imagine similar scenarios that could lead to civil or criminal charges."[118]

Operation Aurora did much to introduce the private sector to the concept of APTs, a term that, like "active defense," was borrowed from the military.[119] In 2011, McAfee defined APTs as "sophisticated, covert attacks bent on surreptitiously stealing valuable data from targeted and unsuspecting companies" and claimed that such "targeted attacks are on the rise."[120] Yet defining APTs may be a malleable and circumstantial exercise—and may even represent a politically or economically minded euphemism. In 2011, for example, the CEO of security firm HBGary said that the definition of an APT varies depending on "who you ask," and the terminology really only emerged because the U.S. Department of Defense and Air Force needed a "nice way" to refer to Chinese state-sponsored threats.[121] Likewise, McAfee has argued that "the motive of the adversary . . . is the primary differentiator of an APT attack from a

[115] Zetter, *supra* note 13.

[116] 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.

[117] *Id.*

[118] Lachow, *supra* note 44, at 9. This episode also helped bolster services like virustotal.com, which allows users to anonymously post viruses, share threat information, and in so doing build trust and demonstrate competence. This forum breeds collaboration among practitioners that can then branch out to organizations, and in so doing can be a more organic (and effective) model of cyber threat information sharing than other formalized regimes.

[119] Elazari, *supra* note 20, at 4, 6-7. According to Elazari, APT terminology "originated in the U.S. Air Force to describe the most sophisticated type of adversary . . . ." Elazari, *supra* note 20, at 7. *But see* Ellen Messmer, *What is an 'Advanced Persistent Threat,' Anyway?* NETWORK WORLD (Feb. 1, 2011), http://www.networkworld.com/news/2011/020111-advanced-persistent-threat.html ("Some claim the term 'Advanced Persistent Threat' originated somewhere in the Defense Department" while a chief security officer said he 'thinks' that it originated in the Air Force.").

[120] *Combating Advanced Persistent Threats*, MCAFEE (2011), http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf, at 3. *See also* Eric M. Hutchins, Michael J. Cloppert, & Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, LOCKHEED MARTIN CORP. 1 (2010), http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (defining APTs as a "new class of threats" describing "well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information.").

[121] Messmer, *supra* note 119.

cybercriminal or hacktivist one" and agrees that APTs are targeted attacks "carried out under the sponsorship or direction of a nation-state for something other than a pure financial/criminal reason or political protest."[122] Yet this statement fails to appreciate that determining which motive dominates can be an even more daunting challenge than establishing attribution.

Even though some industry experts have suggested that "APT hysteria" was overblown, and "*some* who [thought] that they [were] victims of APTs [were] really the victims of organized criminals, hacktivists, glorified script kiddies, and their own mistakes," evidence clearly demonstrates that malware has become more "customized," meaning anything from a simple repackaging of existing malware to "code written from the ground up for a specific attack."[123] By 2013, more security experts claimed that sophisticated, targeted attacks posed the greatest information security "danger" for businesses, that traditional defense technologies were "slowly losing relevance" because they were ineffective, and that companies were increasingly frustrated by attempting to protect themselves "with a purely defensive posture."[124] Indeed, APTs are built to circumvent passive cyber defenses like firewalls and anti-virus software. Private sector actors' self-reporting suggests that most advanced attacks go unnoticed for more than one year (and are often ultimately noticed by a third party); a reasonable conclusion is that APTs often circumvent purely defensive postures.[125]

In the early 2010s, continuing "massive cases of cyber exploitation," including GhostNet, Night Dragon, and Shady RAT, significantly harmed companies and advanced both media exposure and private sector cybersecurity concerns,[126] reinforcing the perception that APTs were the new norm.[127] Moreover, APTs tipped cyber offense-and-defense asymmetry even further in

[122] *Id.*

[123] DATA BREACH INVESTIGATIONS REPORT, VERIZON 5, 30 (2011), *available at* http://www.verizonbusiness.com/resources/reportsrp_data-breach-investigations-report-2011_en_xg.pdf. In addition, more recently, companies have begun to skirt the political implications of APTs by focusing on the technology at issue. *See, e.g.*, *Maginot Revisited* (2015), *supra* note 2, at 6 (stating that, "[f]or brevity, this report uses the term "advanced malware" to describe tools consistent with those used in APT attacks, even if those tools are widely used by other kinds of attackers").

[124] Lachow, *supra* note 44, at 2; Elazari, *supra* note 20, at 5; and McGee, Sabett, & Shah, *supra* note 20, at 2.

[125] Lachow, *supra* note 44, at 2.

[126] *See, e.g.*, Dimitar Kostadinov, *GhostNet – Part I*, INFOSEC INST. (Apr. 24, 2013), http://resources.infosecinstitute.com/ghostnet-part-i/; Tiffany Hsu, *China-Based Hackers Targeted Oil, Energy Companies in 'Night Dragon' Cyber Attacks, McAfee Says*, L.A. TIMES (Feb. 10, 2011), http://latimesblogs.latimes.com/technology/2011/02/chinese-hackers-targeted-oil-companies-in-cyberattack-mcafee-says.html; Michael Joseph Gross, *Exclusive: Operation Shady RAT – Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza*, VANITY FAIR (Aug. 2, 2011), http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109.

[127] For more on both the weapons involved and the private sector response to cyber attacks, see Chapters 3 and 5 of SHACKELFORD, *supra* note 19.

the attackers' favor. Attackers already benefitted from the comparatively small risk of being caught and prosecuted; conversely, defenders already were forced to make significant investments and accept greater risks when deciding how to defend their networks. The rise of APTs enabled attackers to access greater resources and more advanced technologies (such as from a state sponsor or criminal organization) while private sector defenders continued to struggle to increase IT security budgets and employ less sophisticated technologies. According to security expert Keren Elazari in a report prepared for Crowdstrike:

> Simply put, the bad guys are gaining the upper hand. Cybercrime and corporate espionage attackers are persistent—and they only need to get in once . . . . Advanced attackers are using previously unknown zero-day vulnerabilities and self-mutating, evasive, and polymorphic malware while detection rates of existing protection mechanisms are falling. Defenders are facing more malware and more sophistication. Attacks are as lucrative as ever for advanced and commonplace adversaries. Clearly, the time has come for a strategic shift of focus for cybersecurity. Active defense has emerged as the new security paradigm that can help defenders resolve the gap between detection and response and make life more difficult for attackers.[128]

In the face of escalating numbers and sophistication of cyber threats, and the imbalance between attackers and defenders, active defense emerged post-2010 as a practice that allows companies to increase the costs to adversaries attacking them—just as, in the physical world, allowing individuals to engage in self-defense increases the potential costs for would-be attackers, therefore possibly dissuading some attackers. However, even though active cyber defense is increasingly emerging as a sensible or "logical"[129] approach by which the private sector can shift a greater burden to attackers, what has been less clear is how the broader cybersecurity industry is evolving to support more proactive measures. The cybersecurity industry is an essential part of the evolution, as expertise and cybersecurity best practices reside in this space. Part II picks up this debate by couching it in the experience of dozens of cybersecurity companies and then focusing on four case studies before pivoting to consider some of the implications for businesses and policymakers in Part III.

[128] Elazari, *supra* note 20, at 5.

[129] *See* McGee, Sabett, & Shah, *supra* note 20, at 2 ("The logic [of having offensive operations in a cyber toolkit] seems valid—the right to self-defense has existed for hundreds of years in the physical realm; it should have a corresponding construct in the cyber world.").

II. The Private Sector Proactively Defends

The lack of legal clarity surrounding proactive, private sector-led cyber defense may have discouraged companies from adopting proactive defensive measures for some time, but recent studies suggest that more firms are increasingly doing so—perhaps because they perceive few other options for protecting their intellectual property and other sensitive information. According to one 2013 survey of 180 companies, 36 percent of companies have engaged in "retaliatory hacking" at least once.[130] More broadly, specialty cybersecurity firms are starting to publicly offer active defense tools.[131] Before proceeding further, though, a brief definitional exercise is necessary. One of the most challenging aspects of discussing cyber defense mechanisms is that there is "no commonly accepted definition of the term 'active cyber defense.'"[132] So far, our use of the term "proactive cybersecurity" has referred to a wide variety of possible implementations, from hacking back to information sharing. In order to be clear about the scope of our survey of proactive cybersecurity practices, we next add context to our choice of included solutions.

A. Outlining the Spectrum of Proactive Cybersecurity Practices

Early on, in 2003, Dave Dittrich, Research Scientist and Engineer Principal of the University of Washington's Applied Physics Laboratory, noted that active cyber defense includes: local intelligence gathering, the only "clearly legal" activity; remote intelligence gathering; actively tracing the attacker; and actively attacking the hacker.[133] A decade later, in 2013, Irving Lachow, Principal Cybersecurity Engineer at MITRE and Senior Associate at the Center for Strategic and

[130] Lachow, *supra* note 44, at 1.

[131] In addition to boutique security firms, Telos Corporation, an IT consulting company that offers a wide array of information and identity assurance as well as network security solutions and services, has also developed active cyber defense technology. *See Telos: Solutions That Empower and Protect the Enterprise*, TELOS, http://www.telos.com/company/overview/index.cfm (last visited Sept. 17, 2014). According to Telos, "[a]ctive defense isn't a tool or a system. It isn't a process or procedure. It's a new and dynamic way of thinking about protecting your cyber environment." *Active Defense*, TELOS, http://www.telos.com/ managed-services/active-cyber-defense/ (last visited Sept. 17, 2014). As such, Telos' active defense methodology is tailored to the operational environments of its clients, requiring that the company first master clients' systems and their critical information and then ensure that employees have sufficient training to maintain those environments and that information. *Id.* Telos also focuses on "customized, rapidly deployed capabilities," including surveillance of the threat landscape, risk evaluation, continuous monitoring of a client's security posture, and "real-time intrusion detection and incident response to deny the adversary a contested area or objective." *Id.*

[132] Jody Westby, *Caution: Active Response to Cyber Attacks Has High Risk*, FORBES (Nov. 29, 2012), http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

[133] *Id.*

International Studies,[134] acknowledged three more nuanced active cyber defense concepts: detection and forensics (including both "local information gathering" via sources like honeypots and "remote information gathering," which may be achieved by watermarking and tracking stolen documents); deception (i.e., allowing an adversary to steal documents that contain false or misleading information); and attack termination (i.e., severing a connection with an infected computer during an attack or "patching unwitting computers" that are being used to launch attacks).[135] Paul Rosenzweig, former Assistant Director for Policy at the U.S. Department of Homeland Security, consultant, and professional law lecturer, proposes a more robust typology integrating the reason for the proactive defensive action—attribution, prevention, or response—with whether the action of the defender took place in network or out of network.[136] He argues that much of active defense is considered accepted practice, while, in contrast, much of the debate surrounds more controversial hack back actions.[137]

In 2013, in conjunction with CrowdStrike, a proactive cybersecurity company for which we have included a detailed case study below, Israeli security expert Keren Elazari wrote that active cyber defense responses "should be informed by the intelligence gathered at the detection and attribution stages" and include: observation, containment, and sandboxing; intelligence dissemination; and collective defense.[138] Elazari notes that effective intelligence dissemination and collective defense not only limit adversaries' maneuvering room but also enable government partners to pursue trade sanctions, civil litigation, and criminal prosecution.[139] Further, Elazari specified that "'active defense' does not mean hacking back or conducting other activities associated with computer crime" and suggested that, if companies are conducting active defense, then they "should include notices of consent to terms as well as an acceptable use policy for computing resources and networks that are owned and operated by [their] organization[s]" and set up honeypots "in a manner so that unmalicious actors will not accidentally walk into them."[140] In addition, Elazari cited legal instances of active cyber defense, including a

[134] Irving Lachow, CTR. STRATEGIC & INT'L STUD., https://csis.org/expert/irv-lachow (last visited Sept. 17, 2014).
[135] Lachow, *supra* note 44, at 5–7.
[136] Paul Rosenzweig, *A Typology for Evaluating Active Cyber Defenses*, LAWFARE (Apr. 15, 2013), http://www.lawfareblog.com/2013/04/a-typology-for-evaluating-active-cyber-defenses/.
[137] Id. ("[W]e are obsessed with the hard cases and that, if we unpack the question a bit we will find a large swath of areas where agreement is wide spread. We will also, I think, readily identify boundary issues where law and policy have a role to play.")
[138] Elazari, *supra* note 20, at 10–12.
[139] *Id.* at 12.
[140] *Id.* at 15.

university's "court-approved . . . counter hacks when a student used university networks and computers to launch hacking campaigns."[141]

The framework used by Elazari, a security professional, can be compared with the view of Lachow, a policy professional. Both include the security tactics of observation, containment, and sandboxing as active measures; however, Elazari also includes activities like setting up honeypots (or honey tokens[142]), generating callbacks when files are viewed on attackers' machines, setting up "decoys" with "fake crown jewels," and encrypting files with "junk information."[143] Meanwhile, Lachow states that "it seems legal" for a company to take action on its own networks and systems by deploying honeypots, actively tracking adversaries' movements, using deception techniques, watermarking documents, terminating connections with compromised machines, and gathering from and sharing information with other organizations, including government agencies.[144] However, according to Lachow, destroying data or causing harm to computers or servers beyond a company's network "would almost certainly be illegal unless the necessity argument or some other rationale"—like informed consent or gathering information to protect its own proprietary information (while not causing any harm)—"could be used to justify such actions."[145] Ultimately, though, Lachow acknowledged that "[a] legal grey zone" also lies in between "these two endpoints."[146]

To gain insights into commonly accepted and utilized means of proactive security, we reviewed twenty-seven cybersecurity products of twenty-two firms to attempt to establish an industry baseline. We then focus on the "hard cases" of firms or programs that primarily focus on active defense, presenting case studies of Crowdstrike, FireEye, HawkEye, and STRONGARM. We collected evidence from the companies' public self-reporting, as their promotional materials and media reports play an important role in how social phenomena

[141] *Id*. at 16. *See also* Lucian Constantin, *FBI, Microsoft Takedown Program Blunts Most Citadel Botnets*, COMPUTER WORLD (July 26, 2013), https://www.computerworld.com/s/article/9241117/FBI_Microsoft_takedown_program_blunts_most_Citadel_botnets. Elazari also highlighted a case in which a court ruled that a remote search of a student's computer files "was justified under the 'special needs' exception to the Fourth Amendment because the [university's IT] administrator reasonably believed the computer was used to gain unauthorized access to confidential records on a university computer, Elazari, *supra* note 20, at 16.

[142] Honey tokens are "data assets, files, or bits of info that can be accessed by privileged users. If these files are accessed remotely or an attempt to do so is detected, there is a clear indication that an adversary might have access to compromised accounts." *Id*. at 11.

[143] *Id*.

[144] Lachow, *supra* note 44, at 8.

[145] *Id*.

[146] *Id*.

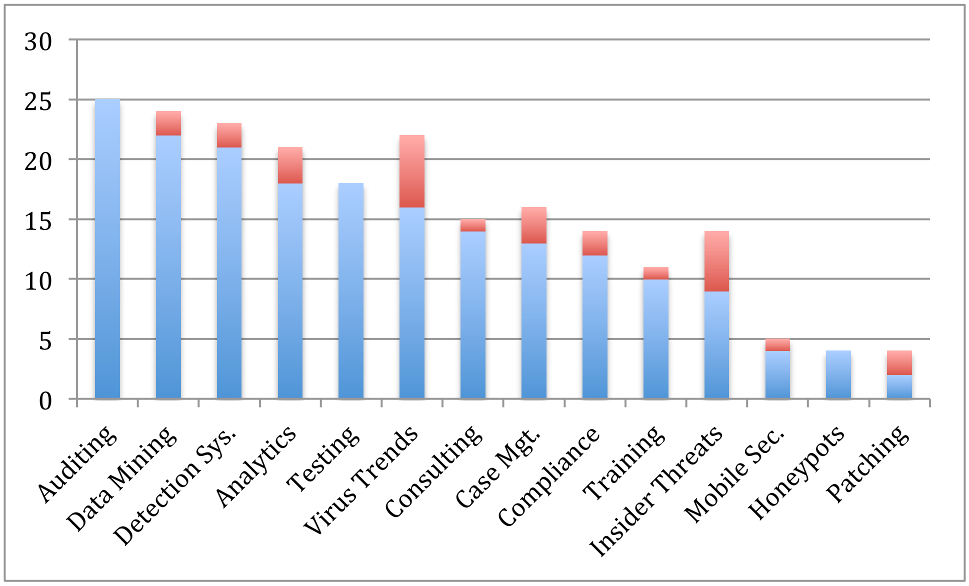
develop, enabling conversations about and affecting perceptions of how the private sector should act and law enforcement should respond.[147]

B. Survey of the Proactive Cybersecurity Industry

To gain an understanding of industry norms that may be emerging, this section reviews the results of a survey of private sector proactive cybersecurity practices. Data resulting from this survey are summarized below in Table 2 and are laid out in greater detail in Appendix B, which shows which companies use or likely use a variety of proactive technologies.

[147] Journalism, which, in today's world of diverse media includes self-reporting (otherwise known in the context of specialty security firms as corporate press releases), has been conceptualized as a social, cultural and political institution, meaning that it interacts with the society in which it is situated. How self-reporting "interacts" helps to define what goals and sociopolitical—including legal—implications it can be expected to produce. The *Ptolemaic Position* and *Copernican* perspectives, representing the worldviews of Ptolemy and Copernicus, differently answer this "how" question. *See* W. Schultz, "Massenmedien und Realität. Die 'ptolemäische' und die 'kopernikanische' Auffassung", *in* MASSENKOMMUNIKATION. THEORIEN, METHODEN, BEFUNDE, OPLADEN, WESTDEUTSCHER VERLAG (1989). The Ptolemaic position "constructs an antagonism between mass media and society," assuming "powerful media effects," and is illustrated by "the formula 'media as a mirror, as a reflection of society.'" Thomas Hanitzsch, *Journalists as a Peacekeeping Force? Peace Journalism and Mass Communication Theory*, 5 JOURNALISM STUD. 483, 438 (2004). According to this position, how specialty security firms depict their own active cyber defense programs may elucidate society's conception of and readiness to accept such programs. Alternatively, the Copernican perspective imagines media as an "active element in the process by which reality is constructed," thus forming an "integral component of society." *Id*. Media and society interact, each communicating to construct its own "reality," so reporting represents "a public negotiation of meaning." Karin Wahl-Jorgensen & Thomas Hanitzsch, *Introduction: On Why and How We Should Do Journalism Studies*, *in* THE HANDBOOK OF JOURNALISM STUDIES 1, 13 (2009). Even in their own reporting, companies must be responsive to public perceptions. As such, according to the Copernican perspective, how specialty security firms depict their own active defense programs may demonstrate how companies and society are negotiating their meaning and legality.

TABLE 2: SNAPSHOT OF PROACTIVE CYBERSECURITY PRACTICES[148]



We created Table 2 with publicly available data drawn from twenty-seven solutions offered by twenty-two companies that promote cybersecurity products, services, or research. The most widespread practices across surveyed companies are on the left side of the chart, while practices on the right side are less common. The stacked column represents those firms that affirmatively state that they offer the pertinent cybersecurity product or service and is followed by, if applicable, an additional column (in red), which shows the number of firms that likely offer that product or service based on interpretations of information available on website marketing and product description materials.

We do not argue that these findings represent definitive industry practice or the positive identification of industry norms, emerging or otherwise. There are hundreds, if not thousands, of firms offering cybersecurity solutions worldwide—so many that some have even questioned whether a cybersecurity bubble is brewing.[149] Still, these findings do represent an industry snapshot (as of October 2014) that offers some telling data points about the areas in which these cybersecurity firms are focusing their efforts. All but one of the surveyed firms (96 percent), for example, offers cybersecurity auditing services, perhaps partly in response to the growing

[148] These data are drawn from Appendix B.
[149] *See* Yoav Leitersdorf & Ofer Schreiber, *Is a Cybersecurity Bubble Brewing?*, FORTUNE (June 14, 2014), http://fortune.com/2014/06/17/is-a-cybersecurity-bubble-brewing/.

importance of the cyber risk insurance industry.[150] Such audits are invaluable in identifying gaps in a company's cybersecurity risk management strategy.[151] This survey also demonstrates that data mining, analytics, and detection systems are being offered by more than 75 percent of the firms investigated. These techniques offer businesses the ability to leverage their own data to identify patterns that could lead to the more robust detection of infiltrators prior to damage being done, especially when that information is married with penetration testing and virus trend analysis (offered by more than 60 percent of these firms).[152]

Looking at the other end of the spectrum, there were also areas of stark divergence among the firms surveyed. Only a handful, for example, offers either independent patching services or honeypots. Even more surprisingly, less than 20 percent of firms offer mobile security solutions, an area of vital importance given the growing prevalence of "bring your own device" programs.[153] Similarly, only about 35 percent of the surveyed firms offer proactive cybersecurity products and services designed to mitigate insider threats. After all, according to Michael DuBose, head of Cyber Investigations at Kroll Advisory Solutions and former chief of computer crime at the U.S. Department of Justice, "amidst all the concern and discussion over foreign hacking, what gets lost is the fact that the vast majority of serious breaches involving trade secrets or other proprietary or classified information are still being committed by insiders."[154] We also expected to see more commonality in the availability of cybersecurity training programs, a bare minimum "proactive" offering. Only 38 percent of surveyed firms offered such programs, even though the majority of firms in a PwC survey recognize that security awareness training is important.[155] Best practice would suggest that cybersecurity

[150] *See, e.g.*, Leigh Thomas & Jeff Finkle, *Insurers in Dash for Expertise to Master Cyber Risk Insurance*, INSURANCE J. (July 14, 2014), http://www.insurancejournal.com/news/national/2014/07/14/334442.htm.

[151] *See* PWC, WHY YOU SHOULD ADOPT THE NIST FRAMEWORK 4 (2014), http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

[152] For more on the rapidly evolving field of cybersecurity analytics, see Cyber Security Analytics, Teradata, http://www.teradata.com/Cyber-Security-Analytics/#tabbable=0&tab1=0&tab2=0&tab3=0&tab4=0 (last visited Nov. 23, 2014); BIG DATA ANALYTICS IN CYBER DEFENSE, PONEMON INST. (Feb. 2013), http://www.ponemon.org/local/upload/file/Big_Data_Analytics_in_Cyber_Defense_V12.pdf.

[153] *See, e.g.*, Tom Canty, *Reducing the Cyber Security Risk for BYOD – Can You Have Your Gadgets and Use Them Too?*, VECTRA (Aug. 1, 2014), http://blog.vectranetworks.com/blog/reducing-the-cyber-security-risk-for-byod.

[154] Brian Fung, *Why Insiders, Not Hackers, Are the Biggest Threat to Cybersecurity*, NAT'L J. (June 10, 2013), http://www.nationaljournal.com/tech/why-insiders-not-hackers-are-the-biggest-threat-to-cybersecurity-20130610.

[155] *See Eye of the Storm: Key Findings from the 2012 Global State of Information Security Survey*, PwC at 5, 23, http://www.pwc.co.nz/global-state-of-information-survey.aspx.

training programs are evaluated early and often—and that their message is regularly reinforced through a firm-wide cybersecurity awareness initiative.[156]

Table 2 provides only a snapshot of the rapidly evolving proactive cybersecurity industry. These data do, however, provide evidence that firms have developed a range of proactive products and services designed to better safeguard their customers from cyber threats. Tracing, Trojan horses, honeypots, and hack back are not new.[157] The prevalence of advanced detection systems, data mining, and analytics products implies that the private sector is undertaking innovative measures based on big data to understand future vulnerabilities, aggregating information to thwart attacks. In order to gain a deeper understanding of how these practices are developing, we next turn to four case studies, beginning with Crowdstrike, to flesh out the current state of several leading private-sector active cyber defense programs.

C. Enter Crowdstrike

In February 2013, Dmitri Alperovitch, who was vice president of threat research at the anti-virus firm McAfee in 2010, announced that CrowdStrike was launching "Falcon, a Big Data Active Defense platform."[158] Alperovitch co-founded CrowdStrike in 2012 and is now the company's Chief Technology Officer.[159] According to co-founder George Kurtz, CrowdStrike was established to "do something" about our fundamentally broken security; he encouraged experts who "have been fighting and responding to nation-state targeted intrusions" to consider joining the company.[160] In a post on his own blog announcing the company's launch, Kurtz wrote that attackers will "always" get past perimeter defenses and alleged that tremendous amounts of intellectual property have been stolen during attacks like Operation Aurora, Night Dragon, and Shady RAT.[161] Moreover, Kurtz wrote, "[a]ttribution is the key strategic piece missing from all existing security technologies" because "[p]rotecting everything is impossible" and "knowing the enemy is the first step" in allocating limited resources.[162] As such, he noted, "[t]he key to

[156] *See* MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 26 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

[157] *See* Deborah Radcliff, *supra* note 51.

[158] Dmitri Alperovitch, *Active Defense: Time for a New Security Strategy*, CROWDSTRIKE (Feb. 25, 2013), http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/.

[159] George Kurtz, *CrowdStrike Launches in Stealth-Mode with $26 Million*, SEC. BATTLEFIELD (Feb. 22, 2012), http://www.georgekurtz.com/2012/02/crowdstrike-launches-in-stealth-mode.html.

[160] *Id.*

[161] *Id.*

[162] *Id.*

success is raising [adversaries'] costs to exceed the value of the data they may be trying to exfiltrate[,] and the only way to accomplish that is by forcing them to change the way they conduct the human-led parts of their intrusions."[163] In other words, whereas attackers can change malware delivery methods cheaply and easily, altering how they identify valuable assets or exfiltrate data is more expensive and time-consuming.

One year later, in launching Falcon, CrowdStrike again highlighted that the industry is "only . . . beginning to grasp . . . the rise of targeted and determined attackers" and that "the traditional passive defense security model . . . is failing. The only option this strategy offers organizations is continuously escalating spending," only "slightly delay[ing] the inevitable compromise," which is achieved at "a fraction of the cost" of passive countermeasures.[164] Citing a July 2011 U.S. Department of Defense announcement, during which the Department said that it will "employ an active cyber defense capability," CrowdStrike announced: "It is time for the private sector to adopt the same strategy, which focuses on raising costs and risks to adversaries in an attempt to deter their activities."[165] Importantly, CrowdStrike next clarified: "Active Defense is NOT about 'hack back', retaliation, or vigilantism . . . we are fundamentally against these tactics."[166] Rather, according to CrowdStrike, an effective proactive cybersecurity strategy (related to our findings in Table 2) should focus on: real-time detection (of adversary intrusion attempts and their unique tradecraft and mission objectives); attribution of threat actors (to understand their identities, intent, and mission); flexibility of response actions (including deception, containment, and tying up adversary resources); and intelligence dissemination (including real-time information sharing with industry partners and government agencies to stop the adversary from attacking others and the employing of civil and criminal prosecution and trade sanctions).[167] Crowdstrike argues that Falcon is the "technology implementation of an Active Defense strategy," available to both enterprises and government agencies.[168] But how does Falcon stack up against other boutique cybersecurity firms' offerings?

D. Focusing on FireEye

[163] *Id.*
[164] Alperovitch, *supra* note 158.
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*

On February 25, 2013—the same day that the Falcon program was announced—FireEye, another boutique cybersecurity firm, announced a new "threat protection platform designed to help enterprises deploy new security models to counter modern cyber attacks."[169] FireEye was incorporated in 2005 by Ashar Aziz, who has been referred to as "one of the best engineers on the planet."[170] After leaving Sun Microsystems, Aziz founded FireEye "to detect and stop APTs" because he believed that APTs represented a "big market opportunity[,]" a problem that was going to get worse, and a problem that would be "extremely difficult to solve."[171] Aziz worked for three years on developing his first product, which uses Virtual Machine Introspection to analyze malicious traffic (that gets past firewalls and other passive defense technologies) and reconstruct attacks so that their inner workings can be better understood.[172] By 2013, FireEye technology was deployed in more than 40 countries in the networks of more than 1,000 governments and companies, including more than one quarter of the Fortune 500.[173]

The threat protection platform that FireEye announced in February 2013 "creates a cross-enterprise threat protection fabric," employing a "broad ecosystem of more than two dozen technology alliance partners."[174] In addition, the platform has three core components: 1) a Multi-Vector Virtual Execution (MVX) Engine, a signature-less[175] threat detection technology specifically intended to "block infiltration mechanisms used by" APTs; 2) a Dynamic Threat Intelligence Cloud, whereby subscribers can "exchange the latest multi-vector threat intelligence on new criminal tactics, developing APT tactics, and malware outbreaks," strengthening collective security; and 3) Threat Intelligence Metadata, which enables interoperability and automation and analyzes malware attributes, actions, and forensics captured by the MVX engine.[176] According to the senior director of security at Splunk Inc., a big data processing

[169] *FireEye Delivers Next-Generation Threat Protection Platform: Multi-Vector Threat Intelligence and Partner Interoperability Create Cross-Enterprise Protection Fabric to Stop Today's Cyber Attacks*, FIREEYE (Feb. 25, 2013), http://www.fireeye.com/news-events/press-releases/read/fireeye-delivers-next-generation-threat-protection-platform [hereinafter *FireEye Delivers*].

[170] Peter Cohan, *FireEye: Silicon Valley's Hottest Security Start-up*, FORBES (May 24, 2012), www.forbes.com/sites/petercohan/2012/05/24/fireeye-silicon-valleys-hottest-security-start-up/.

[171] *Id.*

[172] *Id.*

[173] *FireEye Delivers*, *supra* note 169. *Cf.* Leitersdorf & Schreiber, *supra* note 149 (noting that FireEye has lost most of its value in the latter half of 2014).

[174] *Id.*

[175] Note that most security products utilize "signature-based and pattern-matching technology that today's sophisticated cyber-criminals can easily outsmart." Cohan, *supra* note 170.

[176] *FireEye Delivers*, *supra* note 169.

company,[177] the FireEye platform "can provide attribution as part of your security ecosystem. Splunk software allows a user to take the FireEye data, add context using machine data from other security and business systems, and automate responses as part of an active defense."[178] In addition, a 2014 FireEye brochure contains language that resembles that used by CrowdStrike, asserting that the "traditional security model . . . has collapsed" despite significant IT security investments.[179] However, FireEye does not describe its technology as "active defense," instead focusing on its ability to prevent attacks by understanding an attack's entire lifecycle and sharing intelligence.[180] This is part and parcel of the multi-faceted field of proactive cybersecurity.

E. Hatching HawkEye

In October 2013, Hexis Cyber Solutions unveiled what *Information Week's Dark Reading* called "the industry's first truly active defense solution to detect stealthy advanced cyber threats and take automatic action to remove the threats from the network."[181] After KEYW Corporation, a defense contractor,[182] acquired Sensage in 2012, Hexis was spun off as a commercial products division, having as one of its two primary products HawkEye G, an active defense technology formerly known as Project G.[183] According to KEYW, the company combined Sensage's commercial Project G technology with its own military intelligence expertise to form HawkEye G, which is particularly designed for enterprise customers and "can not only detect threats in real time, but . . . also offer immediate active defense capabilities."[184]

More specifically, HawkEye G can "detect, investigate, remediate[,] and remove threats within the network before they can compromise sensitive data."[185] But Hexis, like Crowdstrike, does not equate active defense with "hacking back"—rather, the company "defines active

[177] *About Us*, SPLUNK, http://www.splunk.com/company (last visited Sept. 18, 2014).
[178] *FireEye Delivers*, *supra* note 169.
[179] *FireEye: Reimagining Security to Prevent, Detect, Contain, and Resolve Today's Advanced Attacks*, FIREEYE (2014), http://www.fireeye.com/resources/pdfs/fireeye-advanced-threat-protection.pdf.
[180] *Id.*
[181] *Hexis Cyber Solutions Launches Intelligent Active Defense Solution*, INFO. WK. DARK RDG. (Oct. 8, 2013), http://www.darkreading.com/hexis-cyber-solutions-launches-intelligent-active-defense-solution/d/d-id/1140624.
[182] Marjorie Censer, *Defense Contractors Translate Their Own Cybersecurity Protections into Business*, WASH. POST (Mar. 17, 2013), http://www.washingtonpost.com/business/capitalbusiness/defense-contractors-translate-their-own-cybersecurity-protections-into-business/2013/03/17/75e7098c-82a6-11e2-b99e-6baf4ebe42df_story.html.
[183] *KEYW Announces the Formation of Hexis Cyber Solutions, Inc.*, GLOBE NEWSWIRE (July 31, 2013), http://investors.keywcorp.com/releasedetail.cfm?ReleaseID=781801.
[184] Javvad Malik, *KEYW Uses Acquired Sensage Technology to Form Hexis Cyber Solutions*, KEYW (Nov. 13, 2013), http://www.keywcorp.com/news/articles/keyw-uses-acquired-sensage-technology-to-form-hexis-cyber-solutions.
[185] *Id.*

defense more closely to how intelligence departments would, as taking action 'within' the enterprise environment against an adversary."[186] As such, Hexis' methodology first detects threats by analyzing large quantities of recent but "historic" data in conjunction with "real-time correlation capabilities."[187] (That is, marrying techniques of big data and real-time cybersecurity analytics discussed in reference to Table 2.) Then, HawkEye G gathers more information to positively identify a threat and removes it (either automatically or manually).[188] Like CrowdStrike and FireEye, Hexis also indicates that sharing threat intelligence information is an integral aspect of its "active defense disruptive technology," listing the integration of threat intelligence under its "detect" stage and sharing threat intelligence under its "remove" stage.[189]

F. Starting STRONGARM

Also in October 2013, MITRE Corporation, a non-profit, partnered with Allied Minds, Inc., a technology capital investment firm, to commercialize STRONGARM, an active defense cybersecurity system.[190] With the aim of commercializing technologies, MITRE operates federally funded research and development centers focused on scientific research and systems engineering.[191] Like FireEye and Crowdstrike, MITRE begins its promotional materials for active cyber defense technology by acknowledging that "[c]yber attacks from advanced actors appear to be growing in scope and increasing in frequency," in part because "current defensive technologies are not well suited to mitigate prolonged and determined attackers leveraging advanced techniques."[192] In addition, MITRE wrote that passive defense technologies "fail to stop advanced attacks and provide no knowledge of what an adversary does once the network is

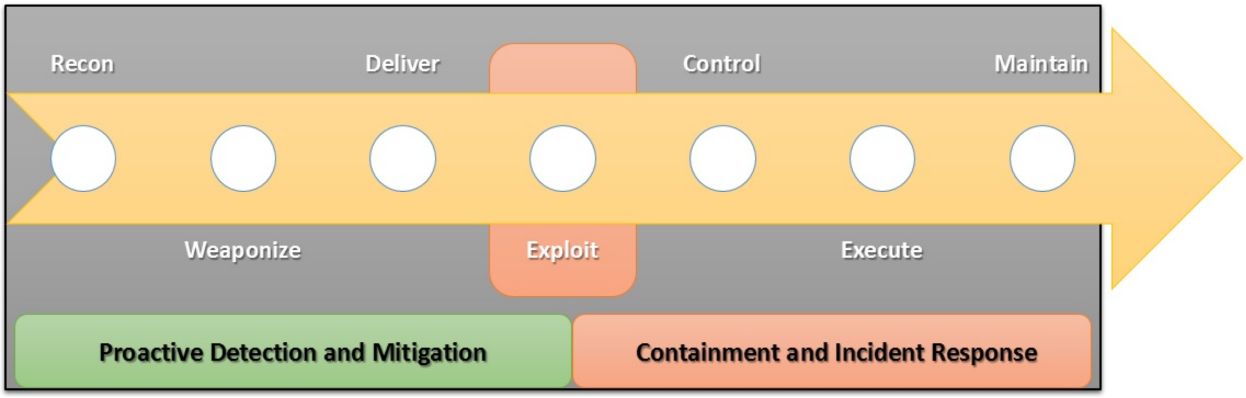
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *HawkEye G: The Active Defense Grid*, KEYW CORP., http://www.keywcorp.com/products/hawkeye-g-the-active-defense-grid (last visited Sept. 18, 2014); *Hexis Cyber Solutions: HawkEye G: The Active Defense Grid*, KEYW CORP., http://www.keywcorp.com/system/products/original/Hexis_HawkEye_G_PS_FINAL.pdf?1375378005 (last visited Sept. 18, 2014).
[190] David Harris, *Allied Minds, MITRE Partnership Means More Funding for Cyber Security*, BOSTON BUS. J. (Mar. 25, 2014), http://www.bizjournals.com/boston/blog/techflash/2014/03/allied-minds-mitre-partnership-means-more-funding.html?page=all; *Allied Minds and The MITRE Corporation Sign Commercialization Agreement to Speed the Pace of Emerging Technologies to Market*, MITRE CORP., http://www.mitre.org/news/press-releases/allied-minds-and-the-mitre-corporation-sign-commercialization-agreement-to-speed (last visited Sept. 18, 2014).
[191] David Harris, *supra* note 190; *Corporate Overview*, MITRE CORP., http://www.mitre.org/about/corporate-overview (last visited Sept. 18, 2014).
[192] *Active Defense Strategy for Cyber*, MITRE CORP. (2012), http://www.mitre.org/sites/default/files/publications/active_defense_strategy.pdf (last visited Sept. 18, 2014).

penetrated."[193] Interestingly, MITRE's partnership with Allied Minds is explicitly aimed at forging "a new process for the smooth and efficient transfer of leading technologies to the commercial marketplace."[194] As such, as private sector companies up their promotion of new, proactive technologies, a federally funded institution has seemingly been given the green light to push that effort forward.

MITRE has shared fewer details about the technical capabilities of STRONGARM technology than Crowdstrike, FireEye, and Hexis have shared about their respective technologies and goals. However, MITRE claims that a "more effective framework for thinking abut cyber defense" than the typical passive defenses, like patching for known viruses and blocking known malicious domain names and IP address, requires considering the "cyber kill-chain."[195] Originally created by Lockheed Martin, this cyber kill-chain—which Lockheed Martin calls an "intrusion kill chain"—depicts seven phases of an incident: reconnaissance (research, identify, and select targets), weaponization (couple remote access Trojan with an exploit into a deliverable payload), delivery (transmission of weapon, e.g. as email attachment), exploitation (intruders' code triggered, e.g. by operating system vulnerability), installation (of a remote access Trojan or backdoor on victim system), command and control (connection between victim system and Internet controller server established), and actions on objectives (e.g., data exfiltration).[196] Figure 1 shows MITRE's reframed cyber kill-chain, still depicting seven phases.[197] MITRE seemingly collapses Lockheed Martin's "exploitation" and "installation" phases into an "exploit" phase and adds a "maintain" phase, which may be described as an objective.[198]

FIGURE 1: MITRE'S CYBER KILL-CHAIN[199]

[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] Hutchins, Cloppert, & Amin, *supra* note 120, at 4-5.
[197] These include recon (adversary develops a target); weaponize (attack form developed); deliver (vulnerability weaponized); exploit (initial attack executed); control (management of initial victims); execute (adversary executes plan); and maintain (long-term access achieved). *Active Defense Strategy for Cyber*, MITRE CORP., *supra* note 192.
[198] *But see* Danny Yadron & Doug Cameron, *Boeing to Exit Commercial Cybersecurity Business*, WALL ST. J. (Jan. 12, 2015), http://www.wsj.com/articles/boeing-to-exit-commercial-cybersecurity-business-1421085602?autologin=y (discussing a relevant cybersecurity merger with Lockheed Martin leading to an exit by Boeing of its cybersecurity business).
[199] *Defensible Security Posture, Part 2*, NIGE THE SECURITY GUY (Jan. 31, 2014), http://nigesecurityguy.wordpress.com/2014/01/.


Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Proactive Detection and Mitigation
Containment and Incident Response

As MITRE writes, the "early steps of the kill-chain," which are those steps to the left of the "exploit" phase at the middle of the figure, "represent an opportunity to proactively defend and mitigate threats before the adversary establishe[s] a foothold."[200] However, according to MITRE, "[t]o best leverage the opportunity for active defense, it is [also] necessary to perform a retrospective analysis of the threat characteristics across the entire kill-chain . . . ."[201] To do so most effectively, "detailed cyber intelligence," best created via information sharing with peer organizations, is necessary—because "[o]nly by understanding adversaries' behavior against a range of targets over a period of time can defenders generate a robust set of adversary tactics, techniques and procedures."[202] Similarly, according to the authors of the Lockheed Martin paper that introduced the intrusion kill-chain, responding to APTs requires "intelligence-driven computer network defense" because such a model enables defenders to "mitigate not just vulnerability, but the threat component of risk, too."[203] Moreover, the authors write:

> The effect of intelligence-driven [computer network defense] is a more resilient security posture. APT actors, by their nature, attempt intrusion after intrusion, adjusting their operations based on the success or failure of each attempt. In a kill chain model, just one mitigation breaks the chain and thwarts the adversary[;] therefore[,] any repetition by the adversary is a liability that defenders must recognize and leverage. If defenders implement countermeasures faster than adversaries evolve, it raises the costs an adversary must expend to achieve [its] objectives.[204]

[200] *Active Defense Strategy for Cyber*, MITRE CORP., *supra* note 192.
[201] *Id.*
[202] *Id.*
[203] Hutchins, Cloppert, & Amin, *supra* note 120, at 1.
[204] *Id.*

In other words, according to the authors, if kill-chain intelligence sharing is implemented effectively, then even APT "aggressors have no inherent advantage over defenders."[205] If this is even sometimes true, then proactive cybersecurity holds the promise of dramatically changing the playing field in favor of targeted entities and individuals.

Intelligence sharing is a vital aspect not only to MITRE's active cyber defense plan but also to the active cyber defense plans of CrowdStrike, FireEye, and Hexis, even though, as briefly referenced above, some forms or aspects of cybersecurity information sharing would benefit from increased legal clarity and enablement—without being subject to legal control; importantly, enabling information sharing is the subject of bills pending in the U.S. Congress as of this writing.[206] Notably, though, CrowdStrike, FireEye, Hexis, and MITRE all distance themselves from the hack back debate and its legal ambiguity. By including language about "tying up adversary resources," CrowdStrike is the only company that even mentions any activity akin to the early to mid-2000s DoS hack back approaches, but elsewhere, CrowdStrike has made clear that it helps "companies do what they can, within their own firewall and within the confines of the law."[207] Instead of engaging in at times murky legal debates, each company has described its program as being focused on actively detecting attacks,[208] stopping them before they are able to execute an intended action (like stealing data), and assessing in detail attackers' behavior. Still, an open question is whether U.S. and other courts will support facets of the proactive cybersecurity movement, especially collective countermeasures. If so, this developing industry would be provided further maneuvering room, which may only be buttressed in the United States and elsewhere by polycentric regulations—as discussed in Part III.

[205] *Id.*

[206] *See* Inserra & Rosenzweig, *supra* note 46. *See also* David Perera, Information Sharing at Top of Obama Cyber Agenda, Politico (Jan. 13, 2015), http://www.politico.com/story/2015/01/barack-obama-cyber-agenda-114236.html#ixzz3Ol1bOJN0 (discussing proposed cybersecurity legislation including information sharing and liability safe harbor provisions). *See also Framework for Cybersecurity Information Exchange*, MICROSOFT (forthcoming) 2015.

[207] Westby, *supra* note 131.

[208] Although actively detecting attacks seems to represent an insignificant defensive improvement, successful detection would represent an extremely valuable leap forward. As Peter Cohan, has written: "You wouldn't get too far trying to drive by looking in the rear view mirror. But since they compare incoming network traffic to a database of previously detected malware, that's what most companies do when it comes to protecting their computer networks . . . . Security today is based on signature-based and pattern-matching technology that today's sophisticated cyber-criminals can easily outsmart. The offense, the cyber-criminals, has essentially outpaced the defense, which is why there are so many high profile cyber-attacks." Cohan, *supra* note 170. In other words, if intelligence sharing enables companies to attempt to identify attackers using more than previously detected malware, signatures, and easily altered patterns, then criminals may be challenged to better obscure themselves—and obscuring something less malleable like their intentions may be very costly to criminals.

G. Summary

This Part has demonstrated how, in the aftermath of Operation Aurora and the recognition that APTs render passive defenses insufficient, organizations like CrowdStrike, FireEye, Hexis, MITRE, and others have attempted to develop the field of proactive cybersecurity. These companies have done so by creating and promoting active cyber defense programs and technologies and articulating justifications based on APTs. Although outstanding legal issues persist,[209] commercial active defense seemingly continues to gain momentum. For instance, in March 2014, Lockheed Martin bought its first cybersecurity provider, commercial cybersecurity firm Industrial Defender.[210] According to a consultant for the company, Lockheed Martin's purchase is indicative of "where it thinks the cybersecurity market is headed."[211] While Lockheed Martin is mainly oriented toward the public sector, "company planners see a vast private-sector market emerging for cybersecurity solutions."[212] Indeed, Industrial Defender aims to help owners of critical industrial infrastructure protect their operations and data against APTs, adding to Lockheed Martin's broader portfolio of "'intelligence-driven' cyber solutions . . . in the commercial marketplace."[213] Considering the practices of the firms surveyed for this section, cybersecurity boutique firms, and powerhouses like Lockheed Martin as contributing to industry trends, Part III next ponders a broader context for the emergence of industry-led security and evaluates its potential impact on cybersecurity and Internet governance policies.

III. GOVERNANCE TRENDS IN INTELLIGENCE-DRIVEN ACTIVE DEFENSE

Thus far, this Article has discussed how the field of commercialized proactive cybersecurity has developed within the global legal environment. This final Part considers the implications of proactive cybersecurity within the following related policy arenas: the emergence of global security assemblages, which have disassembled traditional governance mechanisms and are reassembling new governance structures; the impact of these structures on the development of a polycentric framework, which creates space for self-regulatory initiatives stemming from market

[209] See *infra*, Part I(B).

[210] Loren Thompson, *Lockheed Martin Moves To Dominate Cyber Defense of Electric Grid & Energy Complex*, FORBES (Mar. 14, 2014), http://www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-to-dominate-cyber-defense-of-electric-grid-energy-complex/.

[211] *Id.*

[212] *Id.*

[213] *Id.*

leaders; and, relatedly, the evolving role of the private sector in Internet governance. We also engage with the question of whether a proactive cybersecurity norm may emerge in international law and summarize what all of this might mean for business leaders and policymakers.

A. The Growth of Polycentric Cybersecurity Assemblages

As firms carve out a legal space in which to engage in proactive cybersecurity measures, including detailed threat intelligence sharing with one another (as is happening across an array of sectors, including retail and aerospace)[214] and with government agencies,[215] they may arguably be creating "global security assemblages," or "settings where a range of different global and local, public and private security agents and normativities interact, cooperate and compete to produce new institutions, practices, and forms of security governance."[216] Professors Rita Abrahamsen and Michael Williams demonstrate that, around the world but especially in the United States, private security has become "ubiquitous," even in the day-to-day activities of ordinary life.[217] Considering its ubiquity, this trend should also be understood in the context of transnational private law trends, which suggest that the globalized private sector is increasingly asserting its right (or its responsibility) to self-govern in rapidly evolving arenas, including cybersecurity.[218] However, drawing on Professor Saskia Sassen's work on global assemblages, Abrahamsen and Williams explain that the development of global security assemblages does not represent the simple transferring of public functions to private actors; rather, their development

[214] *See* Aviation Info-Sharing Body Refining Structure Before September Launch, Inside Cybersecurity (July 16, 2014), http://alturl.com/9roi9; Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, __ FLORIDA INT'L UNIV. L. REV. __ (forthcoming 2015).

[215] *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 3, 12 (2009), http://www.insaonline.org/CMDownload.aspx?ContentKey=e1f31be3-e110-41b2-aa0c-966020051f5c&ContentItemKey=161e015c-670f-449a-8753-689cbc3de85e (presenting government involvement, in addition to private-sector participation, as essential to the legitimacy and effectiveness of a public-private partnership for cybersecurity)

[216] Abrahamsen and Williams, *supra* note 16, at 3.

[217] *Id.* at 1. The Untied States hosts the largest private security market in the world; private security representatives reportedly outnumber public police by three to one in the United States. *Id.* at 2.

[218] *See generally* VIRGINIA HAUFLER, A PUBLIC ROLE FOR THE PRIVATE SECTOR: INDUSTRY SELF-REGULATION IN A GLOBAL ECONOMY (2000); ALFRED C. AMAN, ADMINISTRATIVE LAW IN A GLOBAL ERA (1992); Kenneth W. Abbott & Duncan Snidal, *Strengthening International Regulation Through Transnational New Governance: Overcoming the Orchestration Deficit* (TranState Working Paper No. 127, 2008); Fabrizio Cafaggi, *New Foundations of Transnational Private Regulation* (EU Working Paper RSCAS 2010/52, Private Regulations Series-04, 2010), http://privateregulation.eu/wp-content/uploads/2010/12/RSCAS_2010_53.final.pdf.

affects "the relationship between security and the sovereign state, structures of political power and authority, and the operations of global capital."[219]

A broader restructuring beyond the proactive cybersecurity marketplace, a process defined by three steps, enabled the development of global security assemblages. First, since the 1970s, neoliberal economics has dictated that hierarchical, state-centric structures are "bloated" and should instead be horizontally linked as networks (i.e., governments should focus less on direct service provision and more on managing and organizing), justifying the state's privatizing and outsourcing of security functions.[220] Second, increased fondness for punitive approaches to criminal punishment overwhelmed public resources in many instances, creating an opportunity for the private sector to serve the state's incarceration needs, de-identifying security as the exclusive authority of the state, and thereby demonstrating that justice may be a "technical problem amenable to private solution."[221] This viewpoint has arguably been reinforced in the cybersecurity context by the difficulties of relying on traditional justice systems to bring down global cybercrime networks.[222] Third, as security was increasingly recognized as a service that could be bought and sold on a free market—underscoring the sense that it could serve individuals' needs or insecurities—consumers became "to a degree more responsible for their own security," and risk-based thinking and security technologies became more prevalent.[223] Ultimately, security became "a technique" and "a form of expert knowledge that, while specialized, is by no means the sole purview of public (or national) authorities . . . ."[224]

Such a restructuring has created space for private security organizations to grow, and as they have grown, they have interacted and influenced states, especially, in the case of cybersecurity, as states have learned from their expertise—with the 2014 NIST Cybersecurity Framework being a case in point.[225] Meanwhile, as with prison overcrowding, particular aspects of the Internet have encouraged greater private sector involvement; for instance, the Internet developed in mostly private sector hands, and—as discussed above—cybersecurity incidents

[219] Abrahamsen and Williams, *supra* note 16, at 3.
[220] *Id.* at 3-4.
[221] *Id.* at 4-5.
[222] *Cf.* Mark Clayton, *Hacker's Extradition for Cyber Heist: Sign US is Gaining in Cyber Crime Fight*, CHRISTIAN SCI. MONITOR (Aug. 11, 2010), http://www.csmonitor.com/USA/Justice/2010/0811/Hacker-s-extradition-for-cyber-heist-sign-US-is-gaining-in-cyber-crime-fight (reporting on the increase in successful extraditions to fight elements of the cyber threat).
[223] Abrahamsen and Williams, *supra* note 16, at 5.
[224] *Id.*
[225] *See* NIST, *supra* note 12.

have become widespread and costly while jurisdictional and attribution challenges thwart law enforcement efforts. Acknowledging this context helps to explain not only how cybersecurity boutique firms gained traction[226] but also why the emergence of these firms and their proactive cybersecurity strategies should not be seen as merely a short-term reaction to episodes like Operation Aurora or 2014's high-profile breaches. Indeed, we may now be entering an increasingly polycentric era for cybersecurity defined by multi-level, multi-purpose, and multi-sectoral regulatory efforts stemming from public and private sector initiatives that readily spread across borders, generating positive and negative network effects.

Such effects can be understood within the context of polycentric governance, a field that has been championed by Nobel Laureate Elinor Ostrom and Professor Vincent.[227] It challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[228] and examining the extent to which national and private control can in some cases coexist with communal management. As such, polycentric governance overlaps with discussions of security assemblages and regime complexes,[229] but it goes further, envisioning more than simply competing systems of multilevel regulations or "a collective of partially overlapping and non-hierarchical regimes" that vary in extent and purpose.[230] Instead, it may be understood as an effort to marry elements of these interdisciplinary concepts of regime complexes and clusters and security assemblages together under a single conceptual framework to better study multidimensional problems such as cybersecurity. To accomplish this, Professor Ostrom created the Institutional Analysis and Development (IAD) Framework,[231] which holds

[226] *But see* WILLIAM C. CULBERSON, VIGILANTISM: POLITICAL HISTORY OF PRIVATE POWER IN AMERICA (1990) (arguing that private violence is deeply ingrained in U.S. conceptions of popular sovereignty).

[227] For more on this topic, see Chapter 2 of SHACKELFORD, *supra* note 19.

[228] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

[229] *See* Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 CLIMATE L. 395, 412 (2011) (arguing that certain "regime complexes" that exist as a "middle ground" between fully hierarchical and fragmented systems are analogous to polycentric governance).

[230] Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L ORG. 277, 277 (2004). *See, e.g.*, Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010) (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAVIOR & ORG. 273 (2008) (finding "externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate.")).

[231] *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 121 (Eric Brousseau et al. eds., 2012).

lessons for regulating cybersecurity, including cautioning policymakers against occupying the field and crowding out self-regulatory initiatives stemming from market leaders—such as the firms surveyed in Part II.[232] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems"[233] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[234] This reasoning applies not only to questions regarding how best to regulate the field of proactive cybersecurity[235] but also to issues of Internet governance and norm development.

B. The Intersection of Proactive Cybersecurity and Internet Governance

Acknowledging the growth of polycentric cybersecurity assemblage and both the challenges and opportunities that it raises helps to frame questions about how the field of proactive cybersecurity may evolve, impacting not only private cybersecurity strategies but also Internet governance debates. One open question is how global cooperation may be buttressed by proactive cybersecurity. As Part II of this Article detailed, recently publicized active cyber defense programs include clear and oft-repeated language about the sharing of threat intelligence among public and private sector actors. Such an approach may create opportunities to implement "collective defense," an approach articulated by Microsoft Vice President Scott Charney in 2010.[236] According to Charney, on a spectrum of actions that may be taken to defend against cyber threats, collective defense is a moderate approach—more controversial than individual defense, but less controversial than pure active defense and much less controversial than cyber offense.[237] Thus, he suggested that "society needs to explore ways to implement collective defenses" to better protect unknowingly compromised consumers and the larger

[232] *See supra* note 218 and accompanying text.

[233] *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009).

[234] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSPECTIVES ON POLITICS 7, 9 (2011).

[235] For more on this topic, see research on the four modalities of cyber regulation, namely architecture, law, the market, and norms that "may be used individually or collectively" by policymakers, as discussed in ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 28 (2006).

[236] *See* SCOTT CHARNEY, MICROSOFT CORP., COLLECTIVE DEFENSE: APPLYING PUBLIC HEALTH MODELS TO THE INTERNET (2010), go.microsoft.com/?linkid=9746317.

[237] *Id*. at 3.

Internet ecosystem, citing numerous already-existing international, national, and private sector efforts to promote or use collective defense.[238] Moreover, Charney argued that device health can be bolstered by efforts to identify infected devices, including by analyzing and sharing data from sinkholes, network traffic, and product telemetry; then, such data should be used to identify unknowingly compromised device owners *globally*.

As such, Charney has insinuated that global cooperation is necessary to make proactive cybersecurity a reality across platforms and borders, but he also wrote that collective defense "may require coordination across multiple points of control and the sharing of sensitive or even legally protected information."[239] But given the legal issues surrounding information sharing with regard to cyber attacks,[240] how inclusive should collective defense be? For instance, at the national government level, Franklin Kramer, a former assistant secretary of defense and current international security fellow at the Atlantic Council, has encouraged states to work in small groups—with other states with whom they share values and a history of cooperation—to start building confidence and norms around the protection of critical international infrastructure.[241] Kramer, in essence, is calling for a polycentric approach to enhancing cybersecurity and empowering smaller collectives of stakeholders in Internet governance, though he has also acknowledged that "stability will be enhanced as more entities are engaged."[242]

Kramer's sentiments allude to the benefits and drawbacks of bottom-up and top-down approaches of enhancing cybersecurity and strengthening Internet governance mechanisms. For instance, small groups of firms are oftentimes more willing to share more detailed—and more useful—intelligence with a more intimate, trusted group rather than the public writ large.[243] Yet there are drawbacks to this bottom-up form of governance in both the private and public sectors; for example, a highly fragmented system can also "yield gridlock rather than innovation," due, in part, to an insufficient hierarchy.[244] Such systems must "meet standards of coherence,

[238] *Id*. at 4.
[239] *Id*. at 3. *Also see* Janine S. Hiller, *Legal Aspects of a Cyber Immune System,* PROC. OF THE 5TH ANNUAL CONF. ON CYBER CONFLICT 263, 263 (2013) (discussing public and private dynamics of security.
[240] *See supra* note 206 and accompanying text.
[241] Franklin D. Kramer, *Achieving International Cyber Stability*, ATLANTIC COUNCIL 10, 11 (2012).
[242] *Id*. at 13.
[243] Real world examples include the Financial Services Roundtable or partnerships such as InfraGard and the Information Sharing and Analysis Centers ("ISACs"). Joe Waldron, *Comments of VeriSign, Inc, VeriSign Response to NOI 100721305–0305-01*, DEP'T COMM. INTERNET POL'Y TASK FORCE (Sept. 13, 2010), at 2, http://www.nist.gov/itl/upload/VeriSign_Cybersecurity-NOI-Comments-9-13-10.pdf. *See also infra* note 118.
[244] Keohane & Victor, *supra* note 234, at 17.

effectiveness, [and] . . . sustainability," and unclear hierarchy may lead to inconsistency and systemic failures.[245] Alternatively, a broader partnership may mean that fewer companies or governments feel excluded and motivated to form their own, competitive coalitions—when all companies would likely benefit from more shared intelligence from a more diverse set of partners. Moreover, a wider, multi-stakeholder coalition could push international actors that favor a larger government role in global Internet governance to recognize the importance of maintaining a clear—perhaps even leading—role for the private sector. Alternatively, U.S. private sector dominance of a collective defense coalition may perpetuate or even aggravate already existing international frustrations that have developed because, at least according to some, Internet governance has long been unfairly managed by U.S. entities.[246] In addition, if active defense is largely in response to APTs, and "APTs" represent a politically-motivated euphemism, then companies incorporated in countries like China or Russia may be prohibited or discouraged from joining intelligence-sharing collectives with Western firms.[247]

Meanwhile, enabling Western and friendly governments (such as the Five Eyes of the United States, United Kingdom, Canada, Australia, and New Zealand)[248] to participate in a coalition dominated by Western companies will also involve tradeoffs. On the one hand, including government intelligence about APTs might strengthen collective defense,[249] and the U.S. government has already proven helpful to Google in investigating Operation Aurora and to Microsoft in taking down global botnets.[250] On the other hand, if governments participate, then some companies may hesitate to share some intelligence details, and international participation will surely be more limited. One need only view the economic fallout in the wake of revelations from Edward Snowden to understand the calculus of firms with national countries of

[245] *Id.* at 3, 19–20.

[246] For more on this debate, see Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

[247] Notably, not only Chinese and Russian but also American and other governments may prohibit or discourage companies from certain countries suspected of sponsoring APTs to participate.

[248] *See* Hillary Rodham Clinton, *Remarks on the Release of President Obama Administration's International Strategy for Cyberspace*, U.S. DEP'T STATE, May 16, 2011, http://www.state.gov/secretary/rm/2011/05/163523.htm.

[249] *See, e.g.*, Anderson, Lum, & Walha, *supra* note 26, at 12.

[250] Kim Zetter, *Google Asks NSA to Help Secure Its Network*, WIRED (Feb. 4, 2010), http://www.wired.com/2010/02/google-seeks-nsa-help/; Matthew J. Schwartz, *Microsoft, FBI Trumpet Citadel Botnet Takedowns*, Information Week (June 6, 2013), http://www.darkreading.com/attacks-and-breaches/microsoft-fbi-trumpet-citadel-botnet-takedowns/d/d-id/1110261.

incorporation but global clientele.[251] As an alternative to participating in intelligence sharing cooperatives, as Center for Strategic and International Studies Senior Fellow Jim Lewis wrote, governments may more aggressively put to use "diplomatic, trade, and law enforcement tools to create real consequences [for launching APTs] in an environment where consequences have traditionally been so limited as to be nearly invisible."[252] In other words, governments could more actively manage the operating environment for security firms, APT-threatened companies, and victimized individuals through encouraging the growth of a proactive cybersecurity norm focusing first on protecting critical international infrastructure.

There is no perfect forum in a multipolar world; both top-down and bottom-up regulatory approaches have benefits and drawbacks. In the cyber context, focusing on multilateral treaties would help to manage free riders but risk stalling progress given geopolitical divides, whereas relying on bottom-up norm building promises informality and flexibility, promoting experimentation even as the absence of hierarchical control threatens gridlock. A true polycentric approach would be an all-of-the-above effort that includes the best of both worlds, but determining how this could work in practice is challenging given the rapidly changing and increasingly polycentric cybersecurity assemblages around the world. Yet, as has been made clear, neither the public nor the private sector are backing down from their respective roles in shaping this environment, with nations curbing hack back actions and the private sector continuing to innovate despite an oftentimes ambiguous legal environment. This state of affairs looks set to continue for the foreseeable future, and may have been somewhat bolstered by the outcome of the 2014 Global Multistakeholder Conference on the Future of Internet Governance, more colloquially known as NETmundial, which served to solidify the multi-stakeholder status quo of Internet governance that has prevailed since the 1980s.[253] The 2014 ITU Plenipotentiary Conference also demonstrated the staying power of the private sector in contemporary Internet governance,[254] and that power could deepen if proactive cybersecurity goes mainstream across more jurisdictions and is linked with public-private collective defense measures. Over time, it is

[251] *See* James Bambord, *Edward Snowden: The Untold Story*, WIRED (Aug. 22, 2014), http://www.wired.com/2014/08/edward-snowden/.
[252] James Andrew Lewis, *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*, CTR. FOR STRAT. & INT'L STUD. (Mar. 2014), https://csis.org/files/publication/140313_FireEye_WhitePaper_Final.pdf.
[253] *See* Milton Mueller, *NETmundial Moves Net Governance Beyond WSIS*, INTERNET GOVERNANCE PROJ. (Apr. 27, 2014), http://www.internetgovernance.org/2014/04/27/netmundial-moves-net-governance-beyond-wsis/.
[254] *See* Samir Saran, *The ITU and the Unbundling Internet Governance*, COUNCIL ON FOREIGN REL. (Oct. 22, 2014), http://www.cfr.org/internet-policy/itu-unbundling-internet-governance/p33656.

even possible that a proactive cybersecurity norm may emerge, informed through industry best practices—a possibility that we turn to next.

C. An Emerging Norm of Proactive Cybersecurity?

Any discussion of norm development, especially in a dynamic arena like cybersecurity, must be tempered by the fact that the rapid evolution of relevant technology, actors, and environment strains the traditional framework for the creation and dispersion of norms in international law. Generally, the primary sources of international law are treaties, general principles of law,[255] and custom, the latter of which requires evidence of state practice that nations follow because of a sense of legal obligation.[256] In order "for a universal norm of customary law to develop . . . the practice must be fairly general. That is, it must be common to a significant number of states."[257] How much state practice, backed up by *opinion juris*, is required to establish a new norm of customary international law? Depending on the type of norm involved, that state practice needs to be more or less widespread. For new norms, such as those regarding cybersecurity, the standard generally is "virtually uniform" state practice.[258] That is a tall order, to say the least. Nevertheless, because of the practical and political difficulties surrounding multilateral treaty development in the cybersecurity arena, norm creation provides an opportunity to enhance global cybersecurity without waiting for a comprehensive global agreement—which could come too tardily if at all—if consensus can be reached.

Yet despite the "general agreement on a norms-based approach" to enhancing cybersecurity,[259] "even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage[,] and competition for global influence" have created a

[255] *See* LINDA A. MALONE, INTERNATIONAL LAW 27 (2008) ("General principles are losing importance in modern international law" in part because these principles have been incorporated into custom or codified in treaties).

[256] *See* Statute of the International Court of Justice, art. 38, June 26, 1945, 59 Stat. 1055, http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0. Custom will be an increasingly important source of international cyber law going forward given the relative lack of binding law below the armed attack threshold and the political difficulties involved with negotiating new multilateral accords.

[257] MARTIN DIXON, TEXTBOOK ON INTERNATIONAL LAW 34 (7th ed., 2013).

[258] N. Sea Continental Shelf (F.R.G./Den. v. Neth.), 1969 I.C.J. 41, 72 (Feb. 20); *Assessment of Customary International Law*, ICRC, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin (last visited Jan. 29, 2014) ("To establish a rule of customary international law, State practice has to be virtually uniform, extensive and representative."). The link here with private sector action is that industry practices are informing policymaking, such as may be seen with the NIST Framework. In turn, these policies in the aggregate can then shape norms and ultimately international law depending on their uptake by the international community.

[259] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 55 (2011). .

difficult context for cyber norm development and diffusion,[260] and revelations about NSA programs have arguable exacerbated the situation.[261] Consequently, cyber norms must be "clear, useful, and do-able . . . ." if they are to be successful.[262] In the proactive cybersecurity context, as shown in Part II, there is a growing awareness on the part of industry as to the utility of individual active defense practices.

Increasingly, we are also seeing more stakeholders engage in collective proactive cybersecurity measures, as was discussed above. One example of this is Operation SMN, during which a group of private firms engaged in "the first ever-private sponsored interdiction against a sophisticated state sponsored advanced threat group."[263] Ultimately, the group was able to detect and mitigate the damage to some 43,000 infected systems.[264] This development could pave the way for more private-sector led collective defense, potentially resulting in a new industry norm with important implications for businesses and policymakers (especially regarding information sharing).[265] Further, unlike customary international law, the threshold for industry developed norms[266] is far lower than is expected for states. Although the dimensions studied in Table 2 represent merely an industry snapshot, they do reveal potential areas of convergence, such as cybersecurity audits and the real-time analytics of big data. Over time, this could be reflected in

[260] *Id*. at 58.

[261] *See, e.g.*, Roger Hurwitz, *An Augmented Summary of The Harvard, MIT and U. of Toronto Cyber Norms Workshop* 7 (2012), http://citizenlab.org/cybernorms/augmented-summary.pdf ("States today differ in their visions of cyberspace, especially with regard to issues of information access, sovereign authority and sovereign responsibilities. Also, they do not similarly rank the threats or even have the same sets for ranking. China and Russia construe the flows of dissident political information – Internet Freedom, by another name – as a threat and are less concerned than the U.S. about industrial espionage. Consequently, there might be little agreement on where to begin and the specification of norms might be slow and piecemeal.").

[262] Martha Finnemore, *Cultivating International Cyber Norms*, *in* CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 90, 90 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011). *See* Richard A. Clarke, *A Global Cyber-Crisis in Waiting*, WASH. POST (Feb. 7, 2013), http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html?tid=wp_ipad. Over time, a hierarchy of cyber norms may also be established and married with escalating sanctions as is common across a range of international legal instruments. *Cf.* Jure Vidmar, *Norm Conflicts and Hierarchy in International Law: Towards a Vertical International Legal System?*, *in* HIERARCHY IN INTERNATIONAL LAW: THE PLACE OF HUMAN RIGHTS 13, 14 (Erika De Wet & Jure Vidmar eds., 2012) (questioning "whether the jus cogens-based substantive norm hierarchy is more than theoretical.").

[263] OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 4 (2014), http://novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf.

[264] *See id*.

[265] See Janine S. Hiller, *Cyber Conflict: Microsoft, Cybercrime and Botnets*, ----SANTA CLARA HIGH TECH. J. ---- (2014) (chronicling Microsoft's joint efforts with law enforcement and industry partners to takedown botnets).

[266] Ken KASER & DOTTY OELKERS, SPORTS AND ENTERTAINMENT MARKETING 61 (2007). Yet given how quickly the cybersecurity environment is evolving, even delineating what constitutes "average" behavior may be difficult, though the NIST Cybersecurity Framework may be of some help in this regard.

national policies, such as future private sector-led iterations of the NIST Cybersecurity Framework, giving rise to an emerging collective cyber defense norm in state behavior.[267]

There is also the potential to consider the field of proactive cybersecurity, especially in its collective form, not as an arena ripe for the emergence of stand-alone universal norm(s) of behavior but instead forming one component of a network of local, regional, and global cybersecurity norms. For example, a norm of collective active defense may be considered an interstitial norm modifying "'the effects of' primary norms in international law."[268] It could, for example, be considered as a logical extension of other norms, such as a duty to cooperate with a victim nation if an attack occurred through information systems in a state's territory or a duty of care to secure systems and warn potential victims of imminent cyber attacks.[269] If this conceptualization is accurate, then a proactive cybersecurity norm would not be an emerging norm in and of itself but rather a "tool that sets out the existence of already existing principles"—analogous, some argue, to the concept of sustainable development.[270] In such a package of cybersecurity norms, each reinforces the other as part of a polycentric approach to enhancing global cybersecurity.[271] Similarly, rather than a global norm requiring near universal consensus, the analysis in Parts I and II supports the case for considering the field of proactive cybersecurity writ large as an arena of emerging industry norms regulated to a greater or lesser extent through treaties (such as some elements of the Budapest Convention, which has been

[267] The Cybersecurity Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements." NIST, *supra* note 12, at 4.

[268] DIRE TLADI, SUSTAINABLE DEVELOPMENT IN INTERNATIONAL LAW: AN ANALYSIS OF KEY ENVIRO-ECONOMIC INSTRUMENTS 108 (2007).

[269] *See* Eneken Tikk*, Ten Rules of Behavior for Cyber Security,* NATO CCDCOE at 5–6, 8–9 (2011). In the cybersecurity context, defining a standard of cybersecurity care has been something of an uphill battle with myriad jurisdictions coming to different conclusions. *See* John Black, *Developments in Data Security Breach Liability*, 69 BUS. L. 199, 206 (2013) ("Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information . . . those statutes do not define what constitutes reasonable data security."); *see also* Vincent R. Johnson, *Data Security And Tort Liability*, 11 J. INTERNET L. 22, 22 (2008) (stating that the California Security Breach Information Act "leaves no doubt that businesses owe a duty under California law to protect customers' personal information and that customers may recover damages if businesses breach that duty," yet "makes no attempt to define what constitutes 'reasonable security procedures and practices.'"). There is not yet a comprehensive cybersecurity standard of care crystallizing across sectors, but we do see the beginnings of one with regards to negligence, the duty of oversight, and various statutory schemes to protect critical infrastructure. The situation is ripe for clarification. Whether the NIST Cybersecurity Framework may help with this in the U.S. context, or even internationally giving rise to potential local norms related to proactive cybersecurity, remains an area of active debate. For more on this topic see Shackelford et al., *supra* note 12.

[270] TLADI, *supra* note 268, at 108.

[271] *See infra* notes 228–235 and associated text.

ratified by all the G8 members save Russia), giving rise to local norms.[272] To the extent that regional groupings have some success in crafting norms of conduct related to proactive cybersecurity, such as due diligence, these local norms could crystallize and spread, instilling positive network effects and potentially even a norm cascade.[273]

D. Summary and Implications for Businesses and Policymakers

As shown in Part II, we note a commonality of practices across the security industry in offerings of proactive cybersecurity solutions. Across those companies surveyed, for example, the majority offer: vulnerability testing, real-time analytics, data mining analytics, virus trends and update information, detection systems, and cybersecurity audits. Many others offer insider threat detection, case management, and compliance.[274] These practices help to define what constitutes a standard of cybersecurity care and associated due diligence obligations that will be of interest to managers, investors, insurance companies, and, ultimately, consumers. To the extent that these standards become more mainstream, a process that may be catalyzed by the NIST Cybersecurity Framework, they could potentially have important implications for imposition of liability in the event of data breaches. Managers need to be aware of these trends, especially absent Congressional action in the U.S. context, lest they find themselves negligent in the event of a data breach.

On the part of policymakers, we also see something of a consensus across the G8 that "unauthorized access" should be illegal, though exactly what constitutes such an act and whether the systems must have some security measures in place to qualify was less clear.[275] However, this analysis is far from a comprehensive look across the nations surveyed with regard to regulation in place to further proactive cybersecurity. In the U.S. context, the CFAA, a dated instrument that criminalizes the unauthorized access of computer systems, may be compared to the newer, yet voluntary, NIST Cybersecurity Framework, which emphasizes measures related to proactive cybersecurity. Such an emphasis could help to encourage private firms to become market leaders in identifying and spreading cybersecurity best practices. Improvement is clearly needed; only 13 percent of respondents to a 2012 PwC survey that made the survey's "leader

[272] *See* HANS KELSEN, GENERAL THEORY OF LAW AND STATE 326 (2009).
[273] One potential example of this, if it is realized, is the Northeast Asia Peace and Cooperation Initiative (NAPCI). *See* NAPCI, http://tinyurl.com/otz7oww (last visited Nov. 4, 2014).
[274] *See* Appendix B.
[275] *See* Table 1.

cut," a label used to identify respondents that measured and reviewed their cybersecurity policies annually, had "an overall information security strategy in place[,]" analyzed the types of cyber attacks hitting their networks, and had a CISO or equivalent reporting to "the top of the house[.]"[276] Although encouraging the private sector to adhere to such basic cybersecurity best practices is a first step to respond to ever-increasing cyber threats, a next and important step may be crafting proactive cybersecurity industry norms—and resolving the legal and organizational ambiguities that currently may hold such developments back.

CONCLUSION

A mere decade ago, the two-pronged challenges for proactive cybersecurity seemed to be corporate executives' disinterest in funding cyber defenses and legal uncertainty. But in recent years, and in connection with larger trends connected to the growth of polycentric cybersecurity assemblages, the nature of the Internet, and the rise of APTs targeting private enterprise, proactive cybersecurity programs have become mainstream. These programs decidedly do not promote "hack back" approaches; instead, they advocate for advanced threat intelligence sharing and active detection techniques like honeypots, enabling security companies to reasonably predict access attempts by malicious actors rather than guard against already known but easily re-faced malicious traffic. Such an approach represents an opportunity for firms to create broad, collective defense partnerships; however, with whom and how intelligence is shared will impact both the success of those partnerships and how private sector security actors shape evolving polycentric governance structures. At the national level, industry collaboration is impacting the ways in which cybersecurity is being conceptualized and regulated, as was seen in 2014 with the development of the U.S. NIST Cybersecurity Framework. At the global level, inclusive private sector sharing, if effective, may further embed the U.S. model of private sector-led Internet governance, while narrowing nationalistic partnerships that may further frustrate and embolden those states that prefer a larger role for national governments in Internet governance. It is ultimately up to all stakeholders to engage in effective polycentric partnerships to proactively protect vital assets, such as by crystallizing norms surrounding critical infrastructure protection. Only then might we achieve some measure of cyber peace.

[276] *See Eye of the Storm: Key Findings from the 2012 Global State of Information Security Survey*, PwC at 33, http://www.pwc.co.nz/global-state-of-information-survey.aspx.

Appendix A: Sample of Non-G8 National Active Cyber Defense Laws

Country	Title of Law	Year of Law	Relevant Language of Law
Albania	Criminal Code Article 192/b	2001 (amended November 27, 2008)	• Prohibits unauthorized entry or excessing authorized access to a computer system, in whole or in a part, through violation of security measures. This is punished by a fine or imprisonment up to 3 years. • Provides a heightened penalty when done to a military, national security, public order, civil defense, or health computer system, or any other computer system of public importance. The punishment is imprisonment from 3 to 10 years.
Antigua and Barbuda	The Computer Misuse Act • Part II, 3(1) • Part II, 6(1) • Part II, 7(1), (2) • Part II, 10(1)	2006	• Prohibits knowingly and without authority causing a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer. • Prohibits a person from knowingly and without authority (a) securing access to a computer for the purpose of obtaining, directly or indirectly, any computer service. • Prohibits a person from knowingly and without authority (a) interfering with, interrupting, or obstructing the lawful use of a computer; or (b) impeding, preventing access to, or impairing the usefulness or effectiveness of any program or data held in a computer. • Prohibits a person from receiving access to any program or data held in a computer who is not authorized to receive or have access to that program or data, from another person and he knows that that person has obtained that program or data through authorized or unauthorized means
Australia	Criminal Code Act • *Part 10.7, Div. 476(2)* • *Part 10.7 Div. 477 (1)* • *Part 10.7 Div. 478(1)*	1995 (amended May 28, 2013)	• (a) access to data held in a computer; or (b) modification of data held in a computer; or (c) the impairment of electronic communication to or from a computer; or (d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means; by a person is unauthorised if the person is not entitled to cause that access, modification or impairment. • A person is guilty of an offence if the person causes: (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data

			held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and the person knows the access, modification or impairment is unauthorized. • A person is guilty of an offence if: (a) the person causes any unauthorised access to, or modification of, restricted data; and (b) the person intends to cause the access or modification; and (c) the person knows that the access or modification is unauthorised. • Prohibits an unauthorized person from sending by way of a computer system, certain data to gain knowledge of other data for which they are not intended.
Austria	Austrian Criminal Code	2002	• Prohibits an individual from gaining unauthorized data stored in a computer system. • Prohibits an unauthorized person from intending to hear the contents of a message transmitted through a telecommunications or computer system. • Prohibits an unauthorized person from sending by way of a computer system, certain data to gain knowledge of other data for which they are not intended.
Bahamas	Computer Misuse Act • Part II, § 3 • Part II, § 6 • Part II, § 7	2003	• Prohibits any person who, without authority, knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in any computer. • Prohibits any person who knowingly — (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service. • Prohibits any person who, knowingly and without authority or lawful excuse — (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer.
Barbados	Computer Misuse Act	2005	• A person who knowingly or recklessly, and without lawful excuse or justification gains access to the whole or any part of a computer system. • A person who knowingly or recklessly, and without lawful excuse or justification destroys or alters data. • A person who knowingly or recklessly, and without lawful excuse or justification hinders the functioning of a computer

			system. • A person who knowingly and without lawful excuse or justification intercepts by technical means any transmission to, from or within a computer system that is not available to the public. • A person who knowingly uses a computer to perform any function in order to secure access to any program or data held in that computer or in any other computer with the intention to commit an offence involving property, fraud or dishonesty.
Bosnia and Herzegovina	Penal Code for the Federation of Bosnia Herzegovina • Chapter XXXII, Article 396 • Penal Code for the Republica Srpska, Article 238	2008	• Whoever, by an unauthorized access to the electronic data processing system or network, causes the stoppage or disturbance of the work of such system or network • Whoever, without authorization, accesses another's protected computer database and alters, destroys, copies, uses, conceals, publish or enters his data or computer virus or in some other manner renders useless or unavailable another's computer data or programs.
Botswana	• Penal Code, Chapter 8 (Part II, § 4) • Penal Code, Chapter 8 (Part II, § 5)	2007	• Any person who (a) accesses the whole or any part of a computer or computer system, knowing that the access he or she intends to secure is unauthorized; or (b) causes a computer or computer system to perform any function as a result of unauthorized access to such system. • A person commits an offence where such person, knowingly and by any means, without authorization or exceeding the authorization he or she is given (a) secures access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; or (b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer or computer system.
Dominica	• Penal Code (Part II, *§5)*	2005	• A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system.
Ethiopia	• Penal Code (Sec. II, Art. 706)	2005	• Whoever, without authorization, accesses a computer, computer] system or computer network, is punishable with fine. • Whoever, without authorization, accesses a computer, computer system or computer network, and intentionally takes or uses or causes to be used data or computer services.

Fiji	• Penal Code (Part 17, Div. 6, 340) • Penal Code (Part 17, Div. 6, 343)	2009	• A person commits an offence if he or she (a) causes: (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and (b) knows the access, modification or impairment is unauthorised; and (c) intends to commit, or facilitate the commission of, a serious offence against a law (whether by that person or another person) by the access, modification or impairment. • A person commits a summary offence if he or she (a) causes any unauthorised access to, or modification of, restricted data; and (b) intends to cause the access or modification; and (c) knows that the access or modification is unauthorized.
Ghana	• Electronic Transactions Act, §118 • Electronic Transactions Act, §124 • Electronic Transactions Act, §126 • Electronic Transactions Act, §127	2008	• A person who secures unauthorised access or attempts to secure access to a protected system in contravention of a provision of this Act commits an offence. • A person who intentionally accesses or intercepts an electronic record without authority or permission commits an offence. • A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer programme or a component, which is designed primarily to overcome security measures for the protection of an electronic record, or performs any of those functions with regard to a password, access code or any other similar kind of electronic record, commits an offence. • A person who without lawful authority utilises a device or computer programme in order to overcome security measures designed to protect the electronic record or access to it commits an offence.
Jamaica	• Cybercrimes Act (§ 3) • Cybercrimes Act (§ 6)	2010	• A person who knowingly obtains, for himself or another person, any unauthorised access to any program or data held in a computer commits an offence. • A person commits an offence if that person knowingly- (a) secures unauthorised access to any computer for the purpose of obtaining,

			directly or indirectly, any computer service; or (b) without authorisation, directly or indirectly intercepts or causes to be intercepted any function of a computer.
Japan	Law No. 128, Article 3: Unauthorized Computer Access Law	1999	• No person shall conduct an act of unauthorized computer access …
Kenya	Information and Communications Act (*Part VIA 83U*)	2009	• Any person who causes a computer system to perform a function, knowing that the access he has secured is unauthorized, shall commit an offence.
Kiribati	Telecommunications Act • Part 7, § 65 • Part 7, § 66 • Part 7, § 66	2004	• Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer commits an offence. • Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies commits an offence. • Any person who knowingly – (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer; or (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence.

APPENDIX B: "PROACTIVE" CYBERSECURITY PRODUCTS AND SERVICES INDUSTRY MATRIX[277]

Co.	Product/ Service Name	Explanation	Testing	Real-time Analytics	Data Mining/ Analytics	Virus/ Trends	Detection Systems	Systems Mgmt/Auditing	Cyber Security Consulting	Mobile Security	Insider Threats	Patching Services	Case MGMT	Honeypots	Compliance	Cyber Securit Trainin
			Desc.	Desc.	Desc.	Desc.	Desc.	Desc.	Desc.	Desc.	Desc.	Desc.	Desc.		Desc.	Desc.
Westinghouse (Nuclear arm)	Cyber security assessments and systems implementation	Experienced in designing and assessing nuclear systems and assets and provide cyber security support for nuclear utilities.	Yes	Likely	Likely	Likely	Yes	Yes	Yes		Likely	Likely	Likely		Likely	Yes
Kaspersky	Total & Endpoint Security for Business	Anti-malware tools, systems management, data encryption and mobile security.	Yes	Yes	Likely	Yes	Yes	Yes		Yes	Likely	Yes			Yes	
Raytheon	SureView	Insider Threat Monitoring and Enterprise User Audit Management Solution		Yes	Yes	Likely	Yes	Yes		Yes	Yes		Yes		Yes	
Raytheon	CrossView	Cross Domain auditing (Gives a picture of user activity across networks with different classification levels.	Likely	Likely	Yes	Likely		Yes	Likely		Likely	Likely	Likely		Likely	Likely
Raytheon	Convergence	Enterprise visibility and advanced case mgmt	Likely	Likely	Yes	Likely	Yes	Yes		Likely	Yes		Yes			
LogRhythm	SIEM 2.0	Immediate action on real-world issues, such as when suspicious behavior patterns are detected, specific internal or compliance-driven policies are violated, or critical performance thresholds are crossed.	Yes	Yes	Yes	Yes	Yes	Yes			Yes		Yes		Yes	
Verdasys	Digital Gaurdian	Determines which network, system, application and data-level activities are allowed by policies based on session analysis, file sensitivity and the employee's respective usage rights.	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes		Yes			
CounterTack	Scout & Sentinel	Defense and monitoring products		Yes	Yes		Yes	Yes			Yes			Yes		
CounterTack	Stateful Compromise Indicator	Continuous service searching for evidence of an in-progress attack. Provides details needed to disrupt the attack.	Yes	Yes	Yes	Yes	Yes	Yes			Likely		Yes	Yes		
Deloitte	Enterprise Risk Services / Vigilant by Deloitte	Security management, protection, resilience testing services	Yes		Yes	Likely	Likely	Yes	Yes				Likely		Yes	Yes

[277] These data were drawn from each firm's public webpage.

Ernst & Young	Security Analytics	Analysis of external threats, inside risks, and third-party risks. "Development teams" work to understand client situations.			Yes	Yes		Yes	Yes		Yes		Yes			Yes
Booz Allen Hamilton	Cyber4Sight™	Cyber4Sight Threat Intelligence Services provide a critical, continuous data collection, aggregation, and analysis platform that includes real-time predictive threat alerts, human threat intelligence, and global threat trends.	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Likely		Yes		Yes	
Lockheed Martin	Palisade™ (With Cyber Kill Chain)	Cyber intelligence enterprise solution.	Yes	Yes	Yes	Likely	Yes	Yes					Yes			Yes (I Campaig
Lockheed Martin	Cyber Intelligence Professional Services	Managed services for testing and consulting.	Yes		Yes	Yes	Yes	Yes	Yes			Yes	Yes			Yes
IBM	Security Services	Provides expertise, solutions, knowledgeable security specialists, time-tested methodologies and global reach to team with clients to resolve their security needs.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes				Yes	Yes
Accenture	Trusted Application Delivery Services	Accenture delivers "more robust data-centric architectures and help implement security controls for enterprise applications." They develop and delivery trusted applications.	Yes			Yes		Yes	Yes		Yes					
Computer Sciences Corp (CSC)	CyberConfidence™	A practical, comprehensive, and efficient approach to cybersecurity risk management	Yes	Yes	Yes	Yes	Yes	Yes	Yes						Yes	
SAIC	Security Solutions	A range of services offered	Yes	Yes	Yes	Yes	Yes	Yes	Yes						Yes	Yes
Ixia (Breaking Point Systems)	"Cyber Warrior Training Solutions"	Vulnerability testing and ethical hacking.	Yes		Yes	Yes	Likely	Yes								Yes
Fire Eye / Mandiant	Professional Services	Cyber security professional services	Yes	Yes	Yes	Yes	Yes	Yes	Yes				Yes		Yes	Yes
CrowdStrike	Falcon, Professional Services	Identify, respond, monitor, strike methodology	Yes	Yes	Yes	Yes	Yes	Yes	Yes				Yes	Yes		
KPMG	Cyber Security Framework	Information protection, business resilience, technology risk management, data insight		Yes	Yes		Yes	Yes	Yes		Yes		Yes		Yes	Yes (Cyb Gaming

PwC	Couldn't Locate	They perform lots of research and discussion on cyber security, but didn't come across a listing of services.	-	-	Yes	Yes	-	-	Yes	-	-	-	-	-	-	0
Radware	Professional Services	Enterprise solutions (works with many large customers, e.g. IBM, Microsoft, Oracle, SAP)	Yes	Yes			Yes	Yes							Yes	Yes
Radware	Products	Application Development and Network Security Products		Yes	Yes	Yes	Yes	Yes								
Northrop Grumma n	Contract Services (M5)	Mainly research and contracted work to clients		Yes	Yes		Yes	Yes	Yes				Yes		Yes	Yes
Guiang Corp.	Vulnerability testing solutions and help for systems development	Simulation modeling	Yes		Yes		Yes	Yes						Yes		