RETHINKING ACTIVE DEFENSE: A COMPARATIVE ANALYSIS OF PROACTIVE CYBERSECURITY POLICYMAKING

SCOTT J. SHACKELFORD JD, PH.D.,* DANUVASIN CHAROEN,** TRISTEN WAITE,*** & NANCY ZHANG****

ABSTRACT

Although one segment of the proactive cybersecurity debate—e.g., hack back—has long been derided as a policy option carrying with it great risks of escalation, among other concerns, elements within the U.S. Congress and abroad are actively pushing to give companies a freer hand at defending themselves against cyber attackers. This Article compares several of these efforts, focusing on the so-called Graves bill in the United States with the experiences of China, Singapore, Thailand, Australia, and the G7. Given the Republican National Committee's 2016 embrace of active defense principles, even as some firms like FireEye have begun to publicly admit to hacking back, the time has come to take a fresh look at the implications of this regulatory trend for both business integrity and international security.

* Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business.

** Associate Professor, Associate Dean for Academic Affairs, NIDA Business School (Bangkok, Thailand)

*** JD candidate, Indiana University Maurer School of Law.

**** JD candidate, Indiana University Maurer School of Law.

TABLE OF CONTENTS

INTRODUCTION

In the aftermath of the May 2017 WannaCry ransomware attack, which impacted more than 200,000 computers spread across 150 nations,[1] calls regarding the "sorry state" of cybersecurity became louder, leading some to resurrect a now old debate about permitting firms a freer hand in defending themselves from the onslaught of cyber attackers.[2] On its face, such a policy might be sensical, echoing self-defense rationale and responding to the fact that many sophisticated companies are in the best position to know and understand their own defenses, and what they need to do "to protect their customers, networks, and valuable trade secrets."[3] Such sentiments informed Georgia's State Bill 315, which was passed in May 2018 and would have permitted "active defense measures that are designed to prevent or detect unauthorized computer access" until it was vetoed by former Governor Nathan Deal due to its "national security implications and other potential ramifications."[4] Governor Deal's veto statement, issued at the urging of tech firms,[5] serves to highlight that the problems involved in crafting such a policy are manifest, including attribution and escalation,[6] although this has not stopped proponents from pushing the idea forward as

---

[1] *WannaCry ransom notice analysis suggests Chinese link*, BBC (May 29, 2017), http://www.bbc.com/news/technology-40085241 [https://perma.cc/68RG-7Q46].

[2] *See* Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ [https://perma.cc/LVL4-NBDH].

[3] Scott J. Shackelford, *When it Comes to Cyber Security, Passive Defense is Best*, UNDARK (Feb. 19, 2019), https://undark.org/2019/02/19/when-it-comes-to-cyber-security-passive-defense-is-best/ [https://perma.cc/M57J-BNXY]; *see, e.g.*, *Intangible Assets Increase to 84% of the S&P 500's Value in 2015 Report*, BUS. INTANGIBLES (Mar. 11, 2015), http://www.businessintangibles.com/single-post/2015/03/11/Intangible-Assets-Increase-to-84-of-the-SP-500s-Value-in-2015-Report [https://perma.cc/DTL7-AKP3].

[4] Tara Seals, *Georgia Governor Vetoes Controversial Hack-Back Bill*, THREATPOST (May 9, 2018), https://threatpost.com/georgia-governor-vetoes-controversial-hack-back-bill/131822/ [https://perma.cc/L2HG-NU6Q].

[5] Zaid Shoorbajee, *Google and Microsoft ask Georgia governor to veto 'hack back' bill*, CYBERSCOOP (Apr. 27, 2018), https://www.cyberscoop.com/georgia-sb-315-hack-back-google-microsoft/ [https://perma.cc/4SBU-Q9GR].

[6] Veto Number 18 – SB315 (May 8, 2018), https://gov.georgia.gov/press-releases/2018-05-08/deal-issues-2018-veto-statements [https://perma.cc/QG5B-ULUX].

part of the larger movement toward "proactive cybersecurity," both in the United States and indeed around the world.[7]

Proactive cybersecurity is an amorphous field, comprising a wide range of active and passive measures that are often commonly, though not always accurately, referred to as "active defense." While "hacking back" is a lightning rod within this field,[8] it is just one data point in a larger and more dynamic movement, which includes technological, organizational, and legal best practices deep packet inspection to audits promoting defense-in-depth.[9] Going hand-in-hand with this amorphous understanding lies ambiguity with regards to the legality of active defense techniques such as "honeypots" and information sharing that are acknowledged by some governments as best practices.[10] This Article, though, focuses

---

[7] *See* Wolff, *supra* note 2.

[8] *See, e.g.*, Carl Franzen, *Should US companies be allowed to hack China in revenge? New report says yes*, THE VERGE (May 22, 2013), http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back [https://perma.cc/JX7X-FE7X]; *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 [https://perma.cc/9WXW-U7TK]; Tom Field, *To 'Hack Back' or Not?*, BANK INFO. SEC. (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545 [https://perma.cc/7XUH-H8T9] (discussing, among other things, the likelihood of prosecution in the United States for engaging in hacking back).

[9] *See, e.g.*, Orla Cox, *Proactive Cybersecurity – Taking Control Away from Attackers*, SYMANTEC (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [https://perma.cc/3XM6-R369]; 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 [https://perma.cc/8XYL-H3PN]; *Hackback? Claptrap! – An Active Defense Continuum for the Private Sector*, SEC. TODAY, https://sec.today/events/talk/3f45c4ca-98e7-4dcf-959c-86d73e51f8f5/ [https://perma.cc/7QTP-BGW5] ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality.").

[10] *See, e.g.*, EUROPEAN UNION AGENCY FOR NETWORK & INFO. SEC., PROACTIVE DETECTION OF SECURITY INCIDENTS II: HONEYPOTS 17 (2012), https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots [https://perma.cc/7PRY-RNSP] (defining a "honeypot" as a "computing resource, whose sole task is to be probed, attacked, compromised, used or accessed in any other unauthorized way"); 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 [https://perma.cc/P9UL-CZ6L].

on the active defense debate given its continued prevalence among policymakers in the United States and around the world.[11]

Although "hack back" has long been derided as a policy option carrying with it great risks of escalation and enabling industrial espionage, among other concerns,[12] policymakers at the federal and state levels in the United States, and abroad, are actively pushing to give companies a freer hand at defending themselves against cyber attackers.[13] In fact, even as some commentators still call it the "worst cybersecurity policy idea,"[14] the policy has enjoyed remarkable staying power, even rising to the level of being included in the 2016 Republican National Committee (RNC) Platform.[15] An entire industry is being created to help enable interested firms to engage in active defense measures,[16] despite the fact that relatively few commentators—with the notable exception of former Homeland Security Assistant Secretary Stewart Baker—see much benefit in legalizing active defense measures.[17] Moreover, few seem convinced that the policy is even technically desirable given other established techniques for attributing cyberattacks back to their source.[18] There seems to be more agreement, for example, on the need to reign in law enforcement's use of the rather vague Computer Fraud and Abuse Act (CFAA) given a spate of high-profile and

---

[11] For more on the development of the entire proactive cybersecurity field, see Amanda N. Craig, Scott J. Shackelford & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721, 722 (2015).

[12] *See, e.g.*, Josephine Wolff, *Attack of the Hack Back*, SLATE (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html [https://perma.cc/X7E3-ZYCF].

[13] *See id.*; Craig, Shackelford & Hiller, *supra* note 11.

[14] *See* Wolff, *supra* note 12. ("Active defense, for those not familiar with cybersecurity euphemisms, is the polite term for offense. It's meant to convey that you're just protecting yourself, not attacking anyone, even though, of course, you are attacking someone—that's what makes it so "active.").

[15] *See* Paul Szoldra, *This one sentence in the GOP platform has cybersecurity experts freaking out*, BUS. INSIDER (July 21, 2016) , http://www.businessinsider.com/gop-platform-hacking-back-2016 7?pundits_only=0&get_oall_comments=1&no_reply_filter=1 [https://perma.cc/M8FE-G3GF].

[16] *See, e.g.*, Fahmida Y. Rashid, *Legal hack back lets you go after attackers in your network*, CSO (Oct. 24, 2017), https://www.csoonline.com/article/3234661/hacking/legal-hack-back-lets-you-go-after-attackers-in-your-network.html [https://perma.cc/J8F5-QMAE].

[17] *See* Wolff, *supra* note 12.

[18] *See, e.g.*, Joe Uchill, *Rep: Hacking back bill not 'the Wild West,'* THE HILL (May 26, 2017), http://thehill.com/policy/cybersecurity/335294-rep-hacking-back-bill-not-the-wild-west [https://perma.cc/U4T7-GTRF].

controversial prosecutions in recent years.[19] This Article compares several of these efforts, focusing on the Active Cyber Defense Certainty (ACDC) Act proposed in the United States with the experience of China, Singapore, Thailand, Australia, and the G7. Given the Republican National Committee's embrace of active defense principles, even as some firms like FireEye have begun to publicly admit to hacking back, the time has come to take a fresh look at the implications of this regulatory trend for both business integrity and international security especially given that there is a paucity of literature on the topic to date.[20]

The Article is structured as follows. Part I unpacks the multi-faceted cyber threat facing the private sector that has given birth to now renewed calls to permit active defense measures. Part II analyzes the evolution of the active defense debate in the United States, paying particular attention to the ACDC Act including interviews with representations from Congress and the U.S. Chamber of Commerce. Part III compares U.S. effort at reforming active defense with Singapore's proactive cybersecurity policy surrounding the protection of its critical infrastructure, which has now been underway since 2015, along with those of Australia and China. Part IV investigates the policy implications of this research for managers and policymakers, including for the cyber risk

---

[19] *See* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/ [https://perma.cc/HHN7-CJTY].

[20] *Cf.* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1019, n.172 (2018) (citing Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 104 (2014) ("In the United States, scholars have begun to debate the legality of hack back. To date, that examination has focused exclusively on domestic U.S. law. The discussion is inconclusive, though it is probably fair to say that the weight of analysis favors the conclusion that active hack back by private sector U.S. actors violates the Computer Fraud and Abuse Act (CFAA)." (footnote omitted))); Robert Chesney, *Legislative Hackback: Notes: on the Active Cyber Defense Certainty Act Discussion Draft*, LAWFARE (Mar. 7, 2017, 10:30 AM), https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft [https://perma.cc/BAD2-6MN2] (describing the discussion draft of the Active Cyber Defense Certainty Act, proposed by Representative Tom Graves, which would exempt "active cyber defense measures" from liability under the CFAA); Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 581 (2018); Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 196 (2018).

insurance industry, along with the promise of targeted proactive cybersecurity measures to contribute to a polycentric cyber peace.[21]

1. UNPACKING THE CYBER THREAT TO THE PRIVATE SECTOR

A great deal has been written about the evolution of cyberattacks over the past thirty years since the Morris Worm was unleashed back on November 2, 1988.[22] It is not the purpose of this section to rehash this work, but rather to briefly introduce the multi-faceted nature of the cyber threat facing the private sector, which is animating calls for active defense measures.[23] In short, firms of all sizes face a growing list of antagonists online including hacktivists, criminal organizations, economic competitors, and even nation states; indeed, the threat environment is so complex and dynamic

---

[21] *See* Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 77 (Hamadoun I. Touré & Permanent Monitoring Panel on Info. Sec. World Fed'n Scientists eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [https://perma.cc/9XBH-HSMS]. For a more general background on the application of polycentric governance to addressing cybersecurity, see Scott J. Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895 (2015); Amanda Craig, Scott J. Shackelford & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721 (2015); Scott J. Shackelford, Timothy L. Fort & Jamie Prenkert, *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353 (2014); Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1 (2015).

[22] To see the original findings from Cornell on this episode, see TED EISENBERG ET AL., THE COMPUTER WORM, (Feb. 6, 1989), http://simson.net/ref/1989/Cornell_Worm_Report_1989.pdf [https://perma.cc/8VKE-35ST]. Some argue that the first cyber attack was in fact years earlier in 1982 when a gas pipeline in Siberia exploded allegedly as a result of Soviet spies who had stolen software from a Canadian company that had been implanted with a CIA-sponsored logic bomb, resulting in "the most monumental non-nuclear explosion and fire ever seen from space." THOMAS C. REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR 269 (2005).

[23] *See generally* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE, ch. 1 & ch. 4 (2014) (discussing the rise in cyber threat including cybercrime and espionage, analyzing the development and history of cyber conflicts as well as the cybersecurity strategies of the cyber powers, arguing that cyber powers' relying on an exclusively state-centric approach to cybersecurity may be problematic, and suggesting there is need for polycentric governance that includes private-sector engagement along with multilateral collaboration).

that there are growing calls to unleash artificial intelligence (AI) to manage it more effectively.[24]

Hard, verifiable data is difficult to come by in the cybersecurity space given how reticent many firms are to share when they have been breached, and given that, until recently, many governments have not required firms to disclose the details of their breaches.[25] Estimates range greatly, for example, with regards to the overall number of cyber attacks targeting private firms and how much the average data breach is costing companies.[26] According to the Ponemon Institute, the average data breach cost U.S. companies $7 million in 2017.[27] But, depending on the scale of the cyber attack in question, costs can quickly skyrocket—the Equifax breach, for example, will reportedly wind up costing its insurers alone at least $125 million.[28] On average, a recent report from the National Bureau of Economic Research (NBER) found that "[a]fter suffering a breach of customers' personal data, the average attacked firm loses 1.1 percent of its market value and experiences a 3.2 percentage point drop in its year-on-year sales growth rate."[29] Not exactly eye-

---

[24] *See, e.g.*, Alfred Ng, *Stop Cyberattacks. Just Add Robots*, CNET (Sept. 1, 2017, 5:00 AM), https://www.cnet.com/news/cyberattacks-artificial-intelligence-ai-hackers-defcon-black-hat/ [https://perma.cc/6YHX-8M2H] (arguing that AI can help humans deal with cybersecurity more effectively).

[25] *See, e.g.*, SEC. EXCHANGE COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/WJ4A-8PFH]. It is worth noting that the European Union will require such disclosures part of the new Network Information Security (NIS) Directive, see Peter J. Beshar, *How Companies Should Prepare for Europe's New Cybersecurity Rules*, FORTUNE (Aug. 3, 2016), http://fortune.com/2016/08/03/cybersecurity-europe/ [https://perma.cc/58JY-TZNT].

[26] *See, e.g.*, *April 2017 Cyber Attacks Statistics*, HACKMAGEDDON (June 9, 2017), http://www.hackmageddon.com/2017/06/09/april-2017-cyber-attacks-statistics/ [https://perma.cc/9J6E-57ZR].

[27] *Data Breaches Cost US Businesses an Average of $7 Million—Here's the Breakdown*, BUS. INSIDER (Apr. 27, 2017, 11:00 AM), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4 [https://perma.cc/AUE4-EUE9] (noting that these costs include remediation, customer attrition, business disruption, regulatory fines, legal and public relations costs, direct financial costs, notification costs, credit card reissues and identity theft repair/credit monitoring).

[28] *See Equifax Data Breach to Cost Insurers $125 Million: Property Claim Services*, REUTERS (Oct. 2, 2017, 11:01 AM), https://www.reuters.com/article/us-equifax-breach-insurance/equifax-data-breach-to-cost-insurers-125-million-property-claim-services-idUSKCN1C71Y8 [https://perma.cc/KSC5-BXAR].

[29] Shinichi Kamiya et al., *What is the Impact of Successful Cyberattacks on Target Firms?*, (Nat'l Bureau of Econ. Res. Working Paper No. 24409, 2018), http://www.nber.org/papers/w24409 [https://perma.cc/Z8HP-P3LA].

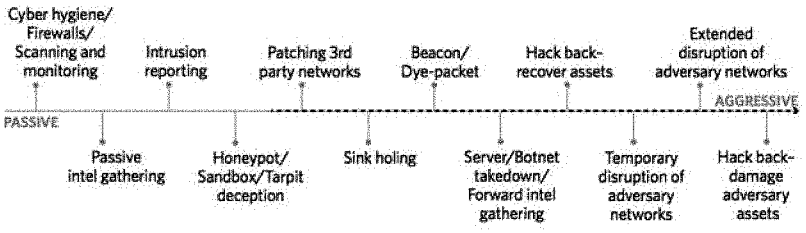
watering figures; in fact, some firms, such as LinkedIn, saw their stock prices actually rise following significant cyber attacks.[30] As a result of such misaligned incentives, proponents like Baker argue that the only way forward is to unleash the power of the private sector to better protect their networks, and vulnerable U.S. critical infrastructure given the fact that more than eighty-five percent of it is owned and operated by companies.[31] The spectrum of active defense options is summarized in Figure 1.

---

[30] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES (June 10, 2012), https://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html [https://perma.cc/X7X6-HR7J] (stating that LinkedIn's stock rose four percent at the end of the week after the breach became public on Wednesday).

[31] *See* Stewart Baker, *Support for Retribution and Active Defense Increases*, STEPTOE (May 22, 2013), http://www.steptoecyberblog.com/2013/05/22/support-for-retribution-and-active-defense-increases/ [https://perma.cc/2SHZ-AVAQ] (arguing that private companies are being encouraged to do more than passively defend their networks); *see also* FEMA, CRITICAL INFRASTRUCTURE 2 (June 2011), https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf [https://perma.cc/B5LT-9V4V] (stating that the private sector owns roughly eighty-five percent of the United States critical infrastructure and key resources).

Figure 1: Active Defense Spectrum[32]



To consider how this idea plays out in practice, let us dive into the example of Shawn Carpenter, who in 2003 was a security analyst at Sandia National Laboratories tasked with investigating a cyber attack on Lockheed Martin.[33] Quickly, Carpenter and his team discovered evidence of Chinese state-sponsored hacking using 'rootkits' to mask their intrusions.[34] Wishing to hold those responsible accountable, Carpenter suggested that the group should hack back at the servers responsible, but leadership at Sandia forbade the attempt since it was in violation of the CFAA, as is discussed in Part II. Instead, Carpenter laid a trap for the attackers by generating honeypots, which are files used to fool hackers, full of faked intelligence documents.[35] Sure enough, they took the bait, and Carpenter followed the hackers back to their source; in the end, "the rabbit hole went much deeper than I imagined."[36] The myriad difficulties Carpenter faced still bedevil active defense proponents to this day, from encryption and attribution issues to spoofing IP

---

[32] *See* WYATT HOFFMAN & ARIEL E. LEVITE, CAN ACTIVE MEASURES HELP STABILIZE CYBERSPACE? 9 (2017), https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf [https://perma.cc/DEE5-YKGA].

[33] *See* Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back [https://perma.cc/8HAU-F6VU].

[34] *Id.*; *see also* Symantec, *Windows Rootkit Overview* 4–6 (2010), http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf [https://perma.cc/9TXZ-DMT6] (explaining that Microsoft rootkits refer to programs that use system hooking or modification to hide programs and behaviors and distinguishing between kernel mode and user mode rootkits).

[35] *See* Schmidle, *supra* note 33.

[36] *Id.*

addresses and the use of virtual private networks (VPNs).[37] But he persisted, and eventually located gigabytes of stolen U.S. defense secrets on a server in South Korea, including plans for the F-22 Raptor and the Mars Reconnaissance Orbiter.[38] Eventually, despite assurances from the FBI, Carpenter was fired for his efforts, though a jury in 2007 awarded him $4.7 million in damages. This test of U.S. legal tolerance for active defense—defining where proactive cybersecurity ends and hacking back begins—helps set the stage for Part II, which unpacks the evolution of this legal concept, along with its current manifestation in the form of the ACDC Act.

2. THE EVOLUTION OF ACTIVE DEFENSE IN THE UNITED STATES

Despite longstanding interest in the field of proactive cybersecurity, the field has been relatively slow to develop. For instance, early examples from the 2000s include efforts on the part of the Motion Picture Association of America (MPAA) to contain the problem of piracy by going after the pirates with distributed denial of service ("DDoS") attacks, Trojan horses, and rootkits.[39] Other examples include "Flash Mobs" targeting fake bank sites.[40] In sum, however, such efforts were limited, fragmented, and relatively unsophisticated. The reasons for this state of affairs are manifold, but include difficulties of attribution, [41] and the fact that cybersecurity was in those times an issue of far less salience and resulting concern to managers and boards of directors contributing

---

[37] *Id.* ("If hackers in Bucharest want to steal from a bank in Omaha, they might first penetrate a server in Kalamazoo, and from there one in Liverpool, and from there one in Perth, and so on, until their trail is thoroughly obscured.").

[38] *Id.*

[39] *See* Robert Anderson, Brian Lum & Bhavjit Walha, *Offense vs. Defense*, 16 (Dec. 11, 2005), http://courses.cs.washington.eu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefense.pdf [https://perma.cc/M4HN-6WTS].

[40] *Flash Mob History*, ARTISTS AGAINST 419, http://wiki.aa419.org/index.php/Flash_Mob_History (last visited Sept. 17, 2014) [https://perma.cc/XT6R-Q79J].

[41] Anderson, Lum & Walha, *supra* note 39, 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.").

to a reactive status quo.[42] But among the biggest barriers, in the United States but also around the world as we will see in Part III, are legal.

2.1. U.S. Regulatory Context for Active Defense Measures

Critics for some time have stated that the "biggest impediment to the deployment" of proactive cybersecurity measures have been legal.[43] For years, a variety of stakeholders including scholars, IT practitioners, and the media have analyzed whether "Internet hack back" represents a form of pragmatic self-defense, or digital vigilantism—a debate that continues to this day.[44] Dig deeper and questions proliferate, such as whether non-malicious third parties should be held liable for related damages.[45] Similarly, the regulation of honeypots is also legally unclear.[46] But among the most important laws regulating this space at the federal level in the U.S.

---

[42] 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.

[43] Anderson, Lum & Walha, *supra* note 39, at 5.

[44] *See, e.g.*, Vikas Jayawal, William Yurcik & David Doss, *Internet Hack Back: Counter-Attacks as Self-Defense or Vigilantism*, IEEE 2002 INT'L SYMP. ON TECH. & SOC'Y (2002), https://ieeexplore.ieee.org/document/1013841 [https://perma.cc/98XA-C2AP] (discussing whether defensive counterattacks with offensive capabilities are appropriate for the civilian/commercial Internet context beyond information warfare); Phil Harris, *Cyber Defense vs. Cyber Vigilante – Part 2 – Hacking Back*, SYMANTEC (July 16, 2013), https://www.symantec.com/connect/blogs/cyber-defense-vs-cyber-vigilante-part-2-hacking-back [https://perma.cc/N847-Q2ZN] (addressing various considerations that may or may not justify hacking back). *See also* Matt Reynolds, *Self-defense in Cyberspace Would Put Businesses at Risk, Experts Say*, MARKET WATCH (July 25, 2019), https://www.marketwatch.com/story/self-defense-in-cyberspace-would-put-businesses-at-risk-experts-say-2019-07-25?mod=hp_econ ("A House bill giving businesses the power to counter cyberattacks outside their own computer networks is fraught with risks to U.S. companies and critical infrastructure, and won't stop criminals and nations from making attacks, experts warn.").

[45] *See* Kenneth Einar Himma, *The Ethics of Tracing Hacker Attacks through the Machines of Innocent Persons*, 2 INT'L J. INFO. ETHICS 1, 1 (2004), http://fiz1.fh-potsdam.de/volltext/ijie/05256.pdf [https://perma.cc/3U3X-Z5D4].

[46] *See* Jerome Radcliffe, *CyberLaw101: A Primer on US Laws Related to Honeypot Deployments*, SANS INST. 19 (2007), https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746 [https://perma.cc/7WBR-3WF8].

context is the 1986 Computer Fraud and Abuse Act ("CFAA"), which we turn to next.

2.1.1. CFAA

The story of the CFAA begins, strangely enough, with a blockbuster movie. In 1983, the movie *War Games* illustrated the potential of hackers to break into the nation's nuclear arsenal. Reagan Administration officials took the threat seriously enough that they worked with Congress to pass the 1986 CFAA.[47] Why is a 1980s era law still so relevant more than thirty years later? The CFAA, as amended in 2008, criminalizes knowing "unauthorized access" of a computer or "unauthorized transmission" of malware, along with "obtaining and trafficking private information, and affecting the use of a computer (such as by using a computer to form a botnet)."[48] One interpretation of the CFAA is that it prohibits companies from accessing networks—even foreign ones due to the law's extraterritorial reach. Under this viewpoint, more passive measures involving the unauthorized access of networks likely do not violate the CFAA.[49] But the global context is also worth keeping in mind as many nations now have similar laws to CFAA in force—as we discuss in Part III below.[50]

Interpretation of the CFAA as applied to hack-back campaigns is an area of active debate. Historically, U.S. law enforcement has taken a dim view of such a "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

---

[47] *See* Schmidle, *supra* note 33.

[48] *See* 18 U.S.C. § 1030 (2008); *see also* 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 [https://perma.cc/YGR5-JZZQ] (defining a botnet as a network of computers working together to perform some task, such as, in the best case, a citizen science project).

[49] *See* CHARLES DOYLE, CONG. RES. SERV., CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS, , 6–7 (2014); Ellen Messmer, *Hitting Back at Cyberattackers: Experts discuss pros and cons*, NETWORKWORLD (Nov. 1, 2012, 12:19 PM), https://www.networkworld.com/article/2161144/hitting-back-at-cyberattackers--experts-discuss-pros-and-cons.html [https://perma.cc/K9GU-QUL8].

[50] Anderson, Lum & Walha, *supra* note 39, at 13–15.

other direction. Just be careful" – because problems still arise when companies "get caught or when innocent bystanders are harmed."[51] As an example of the confusion that has ensued, consider the case in 2000 of Ehippies, which was then a U.K.-based online activist group, that struck at Conxion – a California-based hosting service – with a DoS attack. Conxion could have stopped the incoming traffic in myriad ways, but they decided ultimately to "volley[] them back" at Ehippies' server,[52] actions that were later deemed legal.[53]

The debate continues. Baker has asserted that defenders, for example, who are taking back stolen data may not, in fact, violate the CFAA.[54] Professor Orin Kerr disagrees, taking the view that the CFAA protects computer owners, not data owners.[55] However, although federal-level cybercrime laws with the CFAA being a case in point get most of the attention, it is important not to ignore state-level efforts aimed at improving cybersecurity and regulating hacking back.

2.1.2. State-Level Anti-Hacking Laws

Due to inaction in Congress, states have been experimenting with a range of regulatory interventions designed to provide covered firms with greater certainty about the types of cybersecurity best practices, and active defense policies, permitted by law. These include laws designed to prohibit unauthorized access, similar to the CFAA, along with data breach notification and anti-phishing laws, along with laws designed to decrease the incidents of phishing, DoS

---

[51] *Id.* at 22.

[52] Deborah Radcliff, *Should You Strike Back?*, COMPUTERWORLD (Nov. 13, 2000, 12:00 AM), http://www.computerworld.com/s/article/53869/_Should_You_Strike_Back_?pageNumber=2 [https://perma.cc/R3LG-2WR7].

[53] *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.").

[54] Stewart Baker, Orin Kerr & Eugene Volokh, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ [https://perma.cc/R8JA-9YQ3].

[55] *See id.*

and DDoS attacks, and extortion. The current state of these laws as of June 2018 is summarized in Table 1 and illustrated in Figure 2.

Table 1: Status of State-Level Cybercrime Laws Related to Active Defense[56]

Type of State Law	Coverage	Description
Hacking, Unauthorized Access, Computer Trespass, Viruses, Malware	All 50 States	All fifty states have enacted laws that generally prohibit actions that interfere with computers, systems, programs, or networks.
Data Breach Notification Laws	All 50 States	
Anti-Phishing Laws	23 States: Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Guam	A total of twenty-three states and Guam have enacted laws targeting phishing schemes. Many other states have laws concerning deceptive practices or identity theft that may also apply to phishing crimes.
Anti-Denial of Service/DDoS Laws	25 States: Alabama, Arizona, Arkansas, California,	

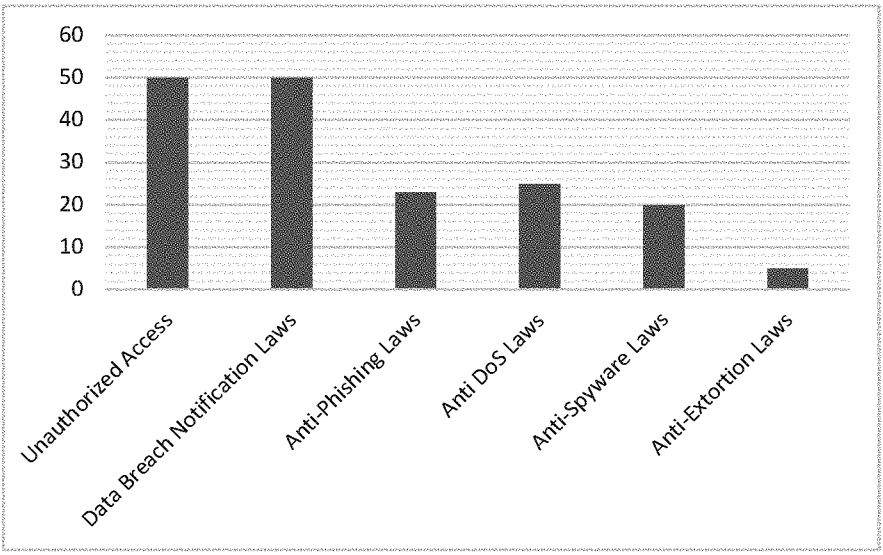
[56] These data have been compiled from the National Conference of State Legislature (NCSL) Report on Computer Crime Statutes (June 14, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking [https://perma.cc/B5EU-DUV5]. It should also be noted that, in addition to these laws, twelve states maintain "data security laws," eight of which include a requirement for firms to implement "reasonable" cybersecurity practices. One example is Indiana. IND. CODE 24-4.9-3-3.5 ("A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."). For more on this topic, see JEFF KOSSEFF, CYBERSECURITY LAW 42–43 (2017). At least thirty-one states also boast data disposal laws that regulate when and how data is destroyed, including the use of "reasonable measures" to ensure that these data are "unreadable or undecipherable[.]" *Id.* at 49.

	Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Mississippi, Missouri, Nevada, New Hampshire, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, West Virginia, and Wyoming	
Anti-Spyware Laws	20 States: Alaska, Arizona, Arkansas, California, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, New York, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, Wyoming, Guam, and Puerto Rico	There are twenty states and two U.S. territories have laws expressly prohibiting use of spyware. Other state laws against deceptive practices, identity theft, or computer crimes in general may be applicable to crimes involving spyware.
Anti-Ransomware Laws/Computer Extortion Laws	5 States: California, Michigan, Connecticut, Texas, and Wyoming	Currently four states have statutes that address ransomware, or computer extortion; however, other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well.

As is evident from these data, states have been making progress in regulating cybersecurity even as Congress has been more hesitant. This may be seen by the spread of data breach notification laws, which now cover all U.S. states, territories, and Washington,

D.C., despite the existence of a single federal standard.[57] Anti-phishing, anti-Do, and anti-spyware laws seem to similarly be reaching a tipping point, with nearly half of U.S. states adopting versions of these prohibitions. However, perhaps surprisingly, only a handful of states have laws tackling the ransomware epidemic sweeping the nation that has impacted everything from hospitals and police departments to municipalities.[58] The balance of these laws is illustrated in Figure 1.

Figure 2: Prevalence of Select State-Level Cybersecurity Laws



As for the substance of these statutes, there are various types of state anti-hacking laws, each of may target specific conduct and computer crimes. However, these laws vary tremendously in form

---

[57] *See, e.g.*, Selena Larson, *Senators Introduce Data Breach Disclosure Bill*, CNN, (Dec. 1, 2017), http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html [https://perma.cc/MZX8-WZG3]. However, with the enactment of the EU's General Data Protection Regulation (GDPR), we may now be seeing a default 72-hour window take effect. *See* Allison Davenport, *CLTC Research: American Companies Struggle to Meet GDPR's Data Breach Notification Rules*, CTR. FOR LONG-TERM CYBERSECURITY (May 16, 2018), https://cltc.berkeley.edu/2018/05/16/cltc-research-american-companies-struggle-meet-gdprs-data-breach-notification-rules/ [https://perma.cc/FT3S-FSUY].

[58] *See* Alfred Ng, *The Global Ransomware Epidemic is Just Getting Started*, CNET (June 28, 2017), https://www.cnet.com/news/petya-goldeneye-wannacry-ransomware-global-epidemic-just-started/[https://perma.cc/KZ3Z-DEU9].

and substance. For example, the state of California has imposed laws aimed at all the types of computer crimes listed above. California's Comprehensive Computer Data Access & Fraud Act, which protects individuals, business, and government agencies from unauthorized access, interference, and damage to computer data and systems, has influenced other states to implement similar anti-hacking laws.[59]

Because California is such a significant norm entrepreneur on state anti-hacking laws,[60] it follows that its jurisdiction is often stricter in the application of its computer crime statutes compared to a state with relatively few computer crime statutes, like Indiana. Indiana Code 35-43-2-3 Computer Trespass makes it a Class A misdemeanor for one to "knowingly" or "intentionally" access a computer, computer system or network without the owner's consent.[61] In Indiana a Class A misdemeanor is punishable up to one year in jail or a fine of up to $5,000.[62] Indiana's computer trespass statute is simpler compared to California's Penal Code Section 502, which includes an extensive list of prohibited computer-related conduct, several definitions of "knowingly," and a variety of punishments that may be imposed. While Indiana has only one general statute prohibiting computer trespass, California is one of the few states that has enacted different statutes specifically targeting the various types of computer crimes. For instance, California is one of just five states to enact anti-ransomware laws, listed in Table 1.[63]

---

[59] Johnathan Levine & Heather Haggarty, *California Online Privacy Laws: The Battle for Personal Data*, 25 J. ANTITRUST, UCL & PRIVACY SEC. ST. B. CAL. 69, 69 (2016); CAL. PENAL CODE §502.

[60] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895-98 (1998) (discussing the potential for norm entrepreneurs to lead to a "norm cascade.").

[61] IND. CODE ANN. § 35-43-2-3 (2009).

[62] However, Indiana is one of only eight states with a reasonable cybersecurity requirement to protect personally identifiable information (PII), as discussed in note 56.

[63] Anti-ransomware laws are still in the early stages of development. On September 27, 2016, Governor Jerry Brown signed Senate Bill 1137, which provided that the use of ransomware is now punishable as extortion. Press Release, Sen. Robert Hertzberg, Gov. Brown Signs Legislation Punishing Ransomware, (Sept. 27, 2016), http://sd18.senate.ca.gov/news/9272016-gov-brown-signs-legislation-punishing-ransomware [https://perma.cc/4YB8-3ZAD]. California Penal Code Section 523(b)(1) states that "[e]very person who, with intent to extort property or other consideration from another, introduces ransomware into any computer,

Although most states are not on California's level regarding cybersecurity regulation, the fact that all fifty states generally prohibit unauthorized access or interference with computer systems, programs, and networks represents a norm cascade of cybersecurity law that is quickly spreading in both scope and scale. Indeed, the EU's 2018 General Data Protection Regulation was modeled, in part, on California's efforts.[64] With time, other states will be able to see the impact of laws enacted by leading influencers in computer crime statutes, like California, and be able to discern how to refine active defense measures within their own respective jurisdictions. Yet this activity has not forestalled federal efforts at similar regulations, which could preempt the norm cascade currently unfolding across the nation, and indeed to an extent, the world. The next section analyzes one of these efforts, including special coverage of how the effort is being viewed by core stakeholders such as the U.S. Chamber of Commerce.

2.2. Analysis of Pending Active Defense Legislation

As of June 2018, Congress was considering a range of cybersecurity legislation, from a privacy bill of rights,[65] to election security,[66] but included in this list is the Active Cyber Defense Certainty (ACDC) Act, also often known as the Graves bill after

---

computer system, or computer network is punishable pursuant to Section 520 in the same manner as if such property or other consideration were actually obtained by means of the ransomware." CAL. PENAL CODE. § 523(b)(1).

64 *See* Laura Sydell, *Do Not Sell My Personal Information: California Eyes Data Privacy Measure*, NPR (May 28, 2018), https://www.npr.org/sections/alltechconsidered/2018/05/28/614419275/do-not-sell-my-personal-information-california-eyes-data-privacy-measure [https://perma.cc/GT54-LWH7].

65 *See* Press Release, Sen. Ed Markey, As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights (Apr. 10, 2018), https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights [https://perma.cc/CU3B-JDT3] ("Specifically, the CONSENT Act: Requires edge providers to obtain opt-in consent from users to use, share, or sell users' personal information; Requires edge providers to develop reasonable data security practices; Requires edge providers to notify users about all collection, use, and sharing of users' personal information; Requires edge providers to notify users in the event of a breach; Requirements are enforced by the FTC.").

66 *See* Martin Matishak, *Lawmakers gather behind election security bill – at last*, POLITICO (Mar. 22, 2018), https://www.politico.com/story/2018/03/22/election-security-bill-congress-437472 [https://perma.cc/9ZCR-H9UT].

Congressman Tom Graves, a Republican from Georgia, whom introduced it. As of June 2018, the bill had nine co-sponsors from both political parties, and even though its imminent passage is unlikely at least in its current form, it received sufficient attention to analyze in some detail.[67] Specifically, the ACDC Act would allow firms to conduct surveillance on entities "who are thought to have done hacking in the past or who, according to a tip or some other intelligence, are planning an attack."[68] The bill also clarifies "the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network."[69] The bill, for example, would permit defendants the ability to claim "that their activities were "active cyber defense measures"[70] so long as they could prove a "persistent unauthorized intrusion" directed at their computers.[71] In summary, according to Congressman Graves, "This is an effort to give the private sector the tools they need to defend themselves[.]"[72]

Part of the impetus for the ACDC Act came from Congressman Graves position as chairman of the financial-services subcommittee of the House Appropriations Committee, in which capacity he was hearing complaints from bank executives who "bought the antivirus software and got all the patches [but] wanted to do more, and had the skills and the tools to do more, but didn't know if they *could*. And some were taking extra steps but didn't know if they *should*."[73] One episode of note in particular involved Iranian attacks on the U.S. banking system, which prompted one bank CEO reportedly to declare at a White House meeting, "Ladies and gentlemen, we are at *war*!"[74] In this instance, U.S. intelligence had known of the attacks in advance, and even know the NSA had warned the FBI in advance, which in turned reached out to the targeted banks, they still were not able to shield themselves completely from the onslaught, and were in fact investigated themselves in the aftermath.[75] Perceptions regarding active defense have changed under the Trump Administration, as seen by former Secretary of Homeland Security Kirstjen Nielsen's support for DHS "to work with the private sector

---

67 *See* Active Cyber Defense Certainty Act, H.R.4036, 115th Cong. (2017-2018).

68 Schmidle, *supra* note 33.

69 Wolff, *supra* note 12.

70 *Id.*

71 *Id.*

72 Schmidle, *supra* note 33.

73 *Id.*

74 *Id.*

75 *Id.*

to deploy active-defense tools against cyberintruders."[76] White House support for active defense has only deepened since former Secretary Nielsen's testimony, especially with the departure of some well-known skeptics, such as former cybersecurity advisor Rob Joyce.[77] The U.S. DoD 2018 Cyber Strategy, for example, calls for a policy of "'defending forward to intercept and halt cyber threats,' including responding with (counter)offensive measures."[78] Indeed, this may be at least partly behind the Trump Administration's decision to not sign up to the Paris Call for Trust and Security and Cyberspace, which included language against hacking back, as is discussed further below.[79]

Concerns regarding the ACDC Act fall across several dimensions, summarized in Table 2. For instance, former NSA Directors Admiral Michael S. Rogers and Keith Alexander, among others, have raised concerns about further destabilization in cyberspace.[80] Others, such as Joyce, were more concerned about "unqualified actors bringing risk to themselves, their targets, and their governments."[81] Representatives from the Justice Department are similarly worried about private actors "[undermining] law-enforcement investigations."[82] And then, of course, there is the specter of attribution that has long loomed large in active defense discussions in particular and cybersecurity generally.[83] A former NSA Deputy Director named Richard Ledgett, for example, has

---

[76] *Id.*

[77] *See* Brian Barrett, *The White House Loses its Cybersecurity Brain Trust*, WIRED (Apr. 16, 2018, 06:56 PM), https://www.wired.com/story/rob-joyce-tom-bossert-white-house-cybersecurity-policy/ [https://perma.cc/4QYE-QL69] (arguing that Rob Joyce's, as well as Tom Bossert's, departure leaves a critical vacancy in American cybersecurity leadership).

[78] Jason Healey, *Getting the Drop in Cyberspace*, LAWFARE (Aug. 19, 2019), https://www.lawfareblog.com/getting-drop-cyberspace [https://perma.cc/3VEB-G7L8].

[79] *See* Louise Matsakis, *The US Sits Out an International Cybersecurity Agreement*, WIRED (Nov. 12, 2018, 07:37 PM), https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/[https://perma.cc/Y3Y4-WNXE] (noting that a number of "major American technology corporations" have endorsed the agreement, even though the US itself has not).

[80] *See* Schmidle, *supra* note 33 (referencing both Rogers' and Alexander's calls to act with caution to avoid escalation when combatting cybersecurity threats).

[81] *Id.*

[82] *Id.*

[83] *See, e.g.*, SHACKELFORD, *supra* note 23, at ch. 6; Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009).

said: "Attribution is really hard. Companies have come to me with what they *thought* was solid attribution, and they were wrong."[84] Ultimately, though, at least from a national security perspective, it is unwarranted escalation that bothers many policymakers and analysts the most since it is so difficult for a private firm to know if they are up against a hacktivist group, criminal syndicate, foreign intelligence service, or a foreign state-owned enterprise. Even Carpenter, whom successfully uncovered the Chinese espionage campaign discussed in Part I, has said: "There's a lot of luck involved . . . Because you don't know what other [intelligence or law enforcement] operations may be going on."[85]

Table 2: Advantages and Disadvantages of Active Defense[86]

Advantages	Disadvantages
More advanced knowledge of potential threats and the attacker's capabilities and intent, which helps to mitigate surprise and protect assets	Backfiring due to human error or manipulation by the attacker
Greater range of options to engage the attacker, including flexibility in where, when, and how	Collateral damage as a result of disrupting or damaging an innocent third party computer or network or wrongly attributing the source of an attack
Enhanced ability to disrupt or shut down a planned or ongoing operation even after the initial penetration of the defender's network	Escalation in an exchange between attacker and defender as a result of the attacker's response to ACD measures
Increased likelihood of deterring future attacks by complicating the attack, impeding the use of data, and	Uncertain strategic implications, including the potential political and legal consequences of

84 Schmidle, *supra* note 33.

85 *Id.*

86 HOFFMAN & LEVITE, *supra* note 32, at 10.

raising the direct and indirect costs to and risk for the attacker (especially in being identified)	measures affecting external networks

Crafters of the ACDC Act are well-aware of these critiques summarized in Table 2, and consequently, built in safeguards. For example, the bill "requires reporting to the FBI-led National Cyber Investigative Joint Task Force before taking active-defense measures, which will help federal law enforcement ensure defenders use these tools responsibly."[87] This would defuse, its proponents argue, any concerns with regards to escalation and attribution.[88] But opinion remains split. For instance, according to Matt Eggers, vice president of cybersecurity policy in the Cyber, Intelligence, and Security division at the U.S. Chamber of Commerce, "the Chamber is continuing to think through its approach to active cyber "D" legislation."[89] Eggers said later that: ""Private entities should not be doing that [engaging in active defense]."[90] Moreover, the bill would mark a substantial push back from the state-level trend discussed above whereby all fifty states have criminalized unauthorized access, and the latest attempt to chip away at these regimes—seen in Georgia, and discussed in the introduction—resulted in a veto. The reintroduction of this bill in 2019 has not altered the politics, despite the most recent version having bipartisan co-sponsors.[91] That does not mean, though, that the debate has been put to rest, the least of which because other

---

[87] Active Cyber Defense Certainty Act, Congressman Tom Graves, https://tomgraves.house.gov/uploadedfiles/acdc_expaliner.pdf [https://perma.cc/3RRM-W74F] (last visited June 26, 2018).

[88] *Id.* at 2 ("These safeguards help ensure that active defense is only targeted at the source of the attack, while imposing a strict standard of care on the defender to ensure that innocent bystanders aren't impact.")

[89] Interview with Matthew J. Eggers, Vice President for Cybersecurity Policy in the Cyber, Intelligence, and Security Division, U.S. Chamber of Commerce (Nov. 19, 2018).

[90] Reynolds, *supra* note 44.

[91] *Id.* (noting that under the 2019 version "Companies could monitor attacks using a 'beacon,' or software that a company could embed in its files so that when its data is stolen, it can trace where the attack is coming from. Under the bill, businesses would inform law enforcement when they take an offensive measure. However, the law would bar the destruction of an attacker's data, or remote access of the attacker's computers.").

jurisdictions are pushing the boundaries of active defense regardless of the official position taken by the federal government.

3. GLOBAL PERSPECTIVES ON ACTIVE DEFENSE: CASE STUDIES ON CHINA, SINGAPORE, THAILAND, AUSTRALIA, AND THE G7

This section globalizes the discussion of active defense with a view toward analyzing how other cyber powers are approaching this same policy debate.[92] The analysis is important for U.S. organizations as well since any hack-back measures they take may run afoul of foreign laws. As such, while this part cannot do justice to the world of cybersecurity regulations pertaining to active defense, it does focus on efforts China, Singapore, Thailand, Australia, and the G7 in hopes of identifying areas of policy convergence and divergence between advanced democracies and fast emerging markets that may be informative to U.S. policymakers and managers.

3.1. China

China has long been proactive in both Internet governance and cybersecurity regulation guided as it is by the concept of "cyberspace sovereignty," which has long been advanced by the Chinese government,[93] and of which active defense strategy is an essential component. This doctrine dates back to at least 2010 when the State Council of China declared its doctrine on cyber sovereignty

---

[92] Lists of cyber powers vary greatly in their composition and methodology. *See, e.g.*, JOSEPH S. NYE, JR., CYBER POWER 5–10 (2010), https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf [https://perma.cc/WW9B-Y972]; Shannon Vavra, *The World's Top Cyber Powers*, AXIOS (Aug. 13, 2017), https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html [https://perma.cc/Y564-FG39].

[93] *See generally* Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 30–34 (2016) (comparing different national approaches to cybersecurity, including China's particularly centralized strategy); Scott J. Shackelford & Frank W. Alexander, *China's Cyber Sovereignty: Paper Tiger or Rising Dragon?*, ASIA & THE PAC. POL'Y SOC'Y (Jan. 12, 2018), https://www.policyforum.net/chinas-cyber-sovereignty/[https://perma.cc/HJ2Y-SBQQ] (discussing China's philosophy that cybersecurity efforts belongs in the hands of the State).

in its "White Paper on the Internet in China," which stated: "The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory, the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected."[94] This paper also set out plans for enhancing cybersecurity and combating cybercrime.[95] However, it was not until 2015 that cyber sovereignty was codified in China under the National Security Law, which evoked active defense "to strengthen network management, prevent, stop and punish cyberattacks, network intrusion, network theft, and dissemination of illegal and harmful information such as cybercrime."[96]

The reason for China's promotion of active cyber defense measures was driven at least in part by its 2015 military strategy,[97] which aimed at winning "informationized local wars" and interpreted "China's commitment to building a cyber force with the capability to engage in offensive asymmetric cyber operations . . . [it described] 'active defense' as adherence to the unity of strategic defense and operational and tactical offense; adherence to the principles of defense, self-defense and post-emptive strike; and adherence to the stance that 'We will not attack unless we are attacked, but we will surely counterattack if attacked.'"[98] As may be seen by this definition, the Chinese use of the "active defense" term falls more on the passive end of the proactive cybersecurity spectrum illustrated in Figure 1. This lack of clarity, discussed further below, complicates international efforts aimed at establishing cybersecurity norms with regards to active defense, similar to foundational differences of opinion over multilateral

---

[94] (国务院新闻办公室网站) [The Internet in China] (promulgated by Information Office of the State Council of the People's Republic of China, June 8, 2010), http://www.scio.gov.cn/zxbd/nd/2010/Document/667385/667385_5.htm [https://perma.cc/4W4A-YTTT].

[95] *Id.*

[96] (中华人民共和国国家安全法) [National Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., July 1, 2015) STANDING COMM. NAT'L PEOPLE'S CONG. GAZ (China).

[97] (中国的军事战略) [China's Military Strategy] (promulgated by Information Office of the State Council of the People's Republic of China, May 26, 2015), http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm [https://perma.cc/4W4A-YTTT] ("China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense . . . ensure national network and information security, and maintain national security and social stability.").

[98] *Id.*

versus multi-stakeholder forms of Internet governance,[99] and the differences between "information security" and "cybersecurity."[100]

Chinese cyber sovereignty and active defense were further reinforced by two national policies in 2016. The first was the National Cyberspace Security Strategy ("Strategy") released on December 27, 2016, which set forth China's positions and propositions on the development and security of cyberspace. The Strategy states nine tasks for the national cybersecurity work at present and in the new future, including the need to safeguard cyber sovereignty, and to crack down on cyber terrorism and crime.[101] The second was the Thirteenth Five-Year Plan for the National Information, published in December 2016 ("Plan"), which serves as an action plan of the Strategy. The Plan states that "[c]yberspace is a new area of national sovereignty. We should build cyberspace protection forces that are commensurate with China's international status and compatible with our cyber power, vigorously develop cybersecurity defenses, locate and defend against cyber intrusions in time, and provide strong backing to safeguarding national cybersecurity."[102] As part of the implementation of the Strategy and Plan, China's controversial Cyber Security Law, which came into force in 2017, was designed to improve cyber sovereignty through data localization and personal data protection. Among other features, the law requires businesses operating critical information infrastructure to store all personal data collected in China within the

---

[99] *See* Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, 16 GEO. J. INT'L AFF. 83, 83 (2015) (distinguishing national approaches to Internet governance, particularly China's commitment to national sovereignty and "multilateral management" as opposed to the U.S.'s support for empowering "a global multi-stakeholder community" to exercise oversight).

[100] *See* Neal Ungerleider, *The Chinese Way of Hacking*, FAST COMPANY (July 13, 2011), https://www.fastcompany.com/1766812/chinese-way-hacking [https://perma.cc/62AM-XVS6] (transcribing an interview with Adam Segal, the Ira A. Lipman Senior Fellow for counterterrorism and national security issues at the Council on Foreign Relations, in which he discusses how the Chinese differentiate between information security and cybersecurity).

[101] (国家网络空间安全战略) [National Cybersecurity Strategy] (promulgated by the Cyberspace Administration of China, Dec. 27, 2016), http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html [https://perma.cc/XKC4-44GJ].

[102] (十三五"国家信息化规划) [Thirteenth Five-Year Plan], (promulgated by the Information Office of the State Council of the People's Republic of China, Dec. 27, 2016), http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm [https://perma.cc/DYD9-AM48].

country.[103] These strategies, plans, and laws provide the Chinese government with "a much freer hand to compel a variety of local and foreign firms to cooperate in law enforcement investigations and protect 'critical information infrastructure.'"[104] Overall, these policies solidify China's march toward both cyber sovereignty—and its efforts to spread this notion globally[105]—and active defense, which will likely guide China's activities in the cybersecurity to a more "managed" Internet in the years to come.[106]

In summary, while the Chinese government has been interested in active defense for more than a decade, there is a lack of clarity and consensus on how the term is used and deployed as a matter of governmental policy when compared to the United States. In fact, China has long outsourced its cybersecurity capabilities employing a diverse range of "patriotic hackers" targeting Western firms and intelligence services.[107] A case in point is the 2018 Marriott hack, which resulted in the theft of over 500 million customer records at around the same time as the Office of Personnel Management (OPM) breach, making 2014 a time of "historic [cyber] assault" on U.S. organizations.[108] In hindsight, such incidents help shine a light on the importance that the Obama Administration placed on securing

---

[103] (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong. Gaz., Nov. 7, 2016, effective June 1, 2016) STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. (China).

[104] Shackelford & Alexander, *supra* note 93.

[105] *See* Evan Osnos, *Making China Great Again*, NEW YORKER (Jan. 8, 2018), https://www.newyorker.com/magazine/2018/01/08/making-china-great-again [https://perma.cc/8356-FGAM] (highlighting cyberspace as an area in which China's global leadership is strengthening in the face of increasing American isolationism).

[106] *See* Scott J. Shackelford, *Welcome to the 'Managed' Internet: Unpacking Cyber-Sovereignty in China's New Cybersecurity Law*, ASIA & THE PAC. POL'Y SOC. (June 15, 2017), https://www.policyforum.net/welcome-managed-internet/[https://perma.cc/Q9CT-X8MD] (explaining that China, along with a number of other countries, are increasingly agreeing on creating an increasingly State "managed" rather than global form of cybersecurity policy).

[107] *See* Guest Blogger for Net Politics, *When China's White-Hat Hackers Go Patriotic*, COUNCIL ON FOREIGN REL. (Mar. 13, 2017), https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic [https://perma.cc/7A3X-HZH5] (noting that China has demonstrated "implicit support" for young hackers' attacking foreign targets, but also seeks to "restrain [the hackers] from undercutting Beijing's overall cyber strategy").

[108] Lily Hay Newman, *If China Hacked Marriott, 2014 Marked a Full-On Assault*, WIRED (Dec. 12, 2018), https://www.wired.com/story/marriott-hack-china-2014-opm-anthem/ [https://perma.cc/R55P-XACF].

the 2015 U.S.-China Cybersecurity Code of Conduct.[109] The agreement may have helped mitigate the bilateral theft of intellectual property in the short term. However, as these practices show no signs of abating and may even be getting worse in the face of ongoing trade tensions,[110] other nations—including Singapore—have begun to push the envelope on proactive cybersecurity.

3.2. Singapore

As with China, Singapore has been a leader in proactive cybersecurity in the Asia-Pacific for years in part due to its status as an epicenter for advanced technologies and finance.[111] In 2014, Singapore allowed private entities to take proactive cyber defense measures by amending its Computer Misuse and Cybersecurity Act. Specifically, it began permitting the government to issue certificates directing "specified persons" to prevent, detect, or counter specific threats to its critical infrastructure, including the financial industry.[112] As of this writing, there has not yet been a public vetting of the performance of this initiative.

To further its active defense efforts, in July 2017, the Cyber Security Agency of Singapore (CSA) released a draft cybersecurity bill for consultation.[113] The Cybersecurity Act was enacted on

---

[109] *See* Ellen Nakashima & Paul Sonne, *China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare*, WASH. POST (June 8, 2018), https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.c86896becdcc [https://perma.cc/52XM-7W3R] (explaining that while China pledged in 2015 not to conduct commercial cyberespionage against the U.S., China does continue engage in some hacking activity against the U.S.).

[110] Lily Hay Newman, *China Escalates Hacks Against the US as Trade Tensions Rise*, WIRED (June 22, 2018), https://www.wired.com/story/china-hacks-against-united-states/[https://perma.cc/BS58-VPK4].

[111] *See, e.g.*, Cung Vu, *Policy Report: Cyber Security in Singapore*, S. RAJARATNAM SCH. INT'L STUD. (Dec. 2016), https://www.rsis.edu.sg/wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singapore.pdf [https://perma.cc/293U-VEQ7] (analyzing the role of technology in the Singapore economy as a driver of the country's investment in cyber security initiatives).

[112] Computer Misuse and Cybersecurity Act, Ch. 50A, pt. 3, § 15(A)(1) (2014) (Sing.).

[113] Wai Ming Yap & Gina Ng, *Singapore Parliament Introduces Cybersecurity Bill*, LEXOLOGY (Feb. 14, 2018),

March 2, 2018. It grants commissioners and investigating officers more powers and tools to investigate and prevent cyber threats, including potentially active defense measures.[114] In the case of any serious and imminent threat to an essential critical infrastructure sector—namely finance, given its outsized role in Singapore's economy[115]—in an emergency the Minister may direct or authorize individuals and organizations to take certain measures or to comply with requirements "as may be necessary to prevent, detect or counter any threat to a computer or computer system or any class of computers or systems or services." [116] Those measures and requirements include, but are not limited to, "requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat," "providing to the Minister or the Commissioner any information . . . obtained from any computer," or specified person, and "providing to the Minister or the Commissioner a report of a breach or an attempted breach of cybersecurity."[117] The specified person would then be immune to civil or criminal liabilities if the actions were performed as required by the commissioners. But if they do not comply, they will be subject to a fine or imprisonment as specified by the Act.[118]

Singapore's active defense initiatives highlight a development mirrored across other nations discussed below. With regard to more aggressive active defense activities such as hack back, the primary concerns discussed above have centered on escalation and attribution. [119] By requiring State authorization, Singapore has

---

https://www.lexology.com/library/detail.aspx?g=64cb1ae1-1306-465a-bfb0-be0679671565 [https://perma.cc/ACD8-LRM4].

114 Cybersecurity Act 2018, No. 9 of 2018 (2018) (Sing.).

115 *See* Gabriel Olano, *Singapore's insurance and finance sector growth to outpace national economy—MAS*, INSURANCE BUS. MAG. (Dec. 14, 2017), https://www.insurancebusinessmag.com/asia/news/breaking-news/singapores-insurance-and-finance-sector-growth-to-outpace-national-economy--mas-87663.aspx [https://perma.cc/PXT6-2XQX] (noting that in 2017, the finance industry was "expected to post a 3.7% growth rate, exceeding the national figure.").

116 Cybersecurity Act 2018, No. 9 of 2018, pt. 4 § 23 (2018) (Sing.).

117 *Id.*

118 *Id.*

119 *See, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 59 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [https://perma.cc/FE8B-TGAN] (noting that "in a State that rigorously monitors Internet use, it is highly unlikely"

enjoyed some of the benefits of using private actors as primary responders to "emergency" cyber threats while taking some measures to maintain accountability. This is similar to how the architects of the ACDC Act envision the role of the FBI in restraining and shaping U.S. firms' active defense efforts.

3.3. Thailand

As with Singapore, cybersecurity has continued to be a preoccupation of the Thai government. In 2018, there were 2,520 incidents reported to Thailand's Computer Emergency Response Team (CERT), including 1102 intrusion attempts and 335 successful intrusions.[120] Firms have become more concerned about their computer systems and data due to this onslaught. Defense-in-depth, including encryption and intrusion detection systems, is central to securing these companies and deterring cyber attacks. And the Computer-Related Crime Act, similar to CFAA, prohibits private firms from going after criminals themselves; active defense in Thailand is generally considered illegal. Section 5 of the Computer-Related Crime Act, for example, indicates that "any person who illegally accesses a computer system for which a specific access prevention measure is not intended for their own use shall be liable to imprisonment not exceeding six months, or a fine not exceeding ten thousand baht, or both."[121] Section 8 states:

> Any person who illegitimately perpetrates any act by electronic means to intercept computer data of other people during its transmission in a computer system and that computer data is not intended for the public interest or for use of general people, shall be subject to imprisonment not

---

that the government is "unaware of an attack group" with significant operational capacities).

[120] *Statistics 2018*, THAI. COMPUTER EMERGENCY RESPONSE TEAM, https://www.thaicert.or.th/statistics/statistics-en.html [https://perma.cc/QB3K-EPJP].

[121] Computer-Related Crime Act, No. 2 B.E. 2560 § 5 (2017) (Thai.), *translated in Thailand's Computer-related Crime Act 2017*, THAI NETIZEN NETWORK (Jan. 25, 2017), https://thainetizen.org/docs/cybercrime-act-2017/ [https://perma.cc/5X3Z-37E7].

> exceeding three years, or a fine not exceeding sixty thousand baht, or both.[122]

Furthermore, Section 25 states that if evidence, including computer data or computer traffic data, has been acquired by illegal means, such evidence cannot be used in courts of law.[123]

Three government officials working in Thai cybersecurity units who wish to remain anonymous were interviewed for this case study. All of them confirmed that "hack back" activities are illegal in Thailand, yet private firms can install defensive mechanisms such as firewalls, IDS, and encryption. However, under a cyber attack, "they are required by law to notify law enforcement agencies. In order to collect evidence of an attack, firms can use honeypots only to collect such evidence and a record of activities, and they need to turn this evidence in to law enforcement in the case of any incident."[124] One of the Thai cybersecurity officials mentioned that in the event of an attack, "companies can protect themselves or stop the attack, for example, by pulling the plug, but they are not allowed to engage any activities that create damage to other networks or computer systems. The defense must not damage any customer data."[125] The Computer Crime Act does not allow a private Thai-based firm to proactively go after hackers. One police officer in the Thai cybercrime unit mentioned that "active defense should be discouraged because this action can create collateral damage to the

---

122 *Id.* at § 8.

123 *Id.* at § 25. Yet, the law in criminal procedure code section 226/1 allows the police or law enforcement to obtain evidence through illegal means, and such evidence can be used in a court of law. This section of the criminal procedure code is normally applied to physical crime. In terms of cybercrime, it is unclear whether this section can be applied. "Where it is appearing to in Court that any evidence arised duly but derived wrongfully, such evidence shall not be admitted by the Court, unless the admission of such evidence will have more useful effect on giving justice than bad effect arisen from an impact on the standard of criminal justice work system or basic right of liberty of people. In consideration of admitting an evidence according to the first paragraph, the Court shall consider all circumstance of case without thinking of the following factors: (1) Proval Value, importance and convincing of evidence; (2) Circumstances and gravity of offence in case; (3) Nature and injury being arisen from the acting in bad faith; (4) A person, doing wrongful act being a cause of deriving the evidence, is punished or not and how it is." Criminal Procedure Code, B.E. 2477 § 226/1, *translated in NATLEX: Database of national labour, social security and related human rights legislation*, INT'L LAB. ORG., http://www.ilo.org/dyn/natlex/docs/MONOGRAPH/93536/109383/F203580879/THA93536%20EngTha.pdf [https://perma.cc/8HNP-GDYQ].

124 Telephone Interview with Senior Official, Thai Electronic Transactions Development Agency, in Bangkok, Thai. (Nov. 9, 2018).

125 *Id.*

network and other computer systems."[126] One of the senior police officers interviewed who specializes in cybercrime investigations mentioned that "computer networks involve many jurisdictions and active defense can violate other nation's laws," a topic returned to below.[127] When asked if there was any possibility of having regulations for active defense, another Thai government official mentioned that "the initiative must come from international agreement or regulations from organizations such as the United Nations or Interpol, and there is a need to have regulations that cover the scope of active defense."[128] If anything, with the Paris Call being a case in point, the international community seems to be turning away from such a permissive regime save, perhaps, for elements within the United States and Singapore as is discussed further in Part IV.

In summary, Thai law allows companies to maintain passive defensive mechanisms within their own systems. The law prohibits hacking back or other aggressive active defense measures shown in Figure 1 that damages third party computer systems, similar to the CFAA approach. Even though Thai law might be amended if international guidelines are introduced concerning active defense, this seems unlikely, especially given the Australian and G7 approaches to proactive cybersecurity outlined below.

3.4. Australia

As stated in Australian Cyber Security Center's 2015 Threat Report, the cyber threat faced by Australia is "undeniable, unrelenting, and continues to grow."[129] But unlike China, Singapore, or Thailand, Australia has long embraced a more bottom-up approach to cybersecurity risk management emblematic in its receptive stance to the National Institute for Standards and

---

[126] Telephone Interview with Police Colonel, Royal Thai Police, Cybercrime Unit, in Bangkok, Thai. (Nov. 9, 2018).

[127] *See infra* Part III(E).

[128] Telephone Interview, Police Inspector, Royal Thai Police, Cybercrime Unit, in Bangkok, Thai. (Nov. 5, 2018).

[129] AUSTRALIAN CYBER SEC. CTR., ACSC 2015 THREAT REPORT 2 (2015), https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2015.pdf [https://perma.cc/7GQY-J6GQ].

Technology Cybersecurity Framework (NIST CSF).[130] To help protect its public sector, Australia opened the Cyber Security Centre in 2014 and established the Australian Cybercrime Online Reporting Network, allowing individuals to report cybercrimes that breach Australian law.[131]

As for specific provisions of Australian law, the broad Privacy Act impacts all companies with revenues of more than $3 million annually.[132] The Act includes a "data security principle," which requires entities that hold personal information to take "such steps as are *reasonable* in the circumstances to protect the information" and to delete information that is no longer relevant for any purpose.[133] Moreover, the Australian Criminal Code prohibits "any unauthorized access to data held in a computer."[134] As of this writing, only the Australian military enjoys aggressive active defense responsibilities but, like the U.S. case study, there have been proposals to change the status quo and free up the private sector to protect their own networks.[135] It is worthwhile to couch these case

---

130 *See* Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L. J. 217, 252 (2016), https://blj.ucdavis.edu/archives/vol-16-no-2/bottoms-up.html [https://perma.cc/D5AH-YC7F] ("This updated Australian cybersecurity strategy is believed to be incorporating elements of the NIST framework . . . [t]his would allow private companies to determine the appropriate level of cybersecurity for their business needs and risk tolerance.").

131 COMMONWEALTH OF AUSTL., AUSTRALIA'S CYBER SECURITY STRATEGY 29 (2016), https://cybersecuritystrategy.pmc.gov.au/index.html [https://perma.cc/NGV2-VQ3M] (last visited Feb. 20, 2018).

132 *Privacy Act 1988* (Cth) Part II, div. 1, § 6D (Austl.).

133 *Privacy Fact Sheet 17: Australian Privacy Principles*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (Jan. 2014), https://www.une.edu.au/about-une/leadership/governance/une-legal-and-governance/privacy?a=63745 [https://perma.cc/Q6XR-RG8W] (emphasis added). However, Australia also imposes data retention requirements in certain circumstances. *See, e.g.*, Josh Taylor, *Mandatory Data Retention Passes Australian Parliament*, ZDNET (Mar. 26, 2015), http://www.zdnet.com/article/mandatory-data-retention-passes-australian-parliament/ [https://perma.cc/96L5-9J7W] (listing cases in which Australia has imposed data retention requirements).

134 Criminal Code Act 1995 (Cth) pt 10.7 s 477.1 (Austl.).

135 *See* Marcus Thompson, *The ADF and Cyber Warfare*, 200 AUSTRALIAN DEF. FORCE J. 43, 43–44 (2016), https://www.defence.gov.au/ADC/ADFJ/Documents/issue_200/Thompson_Nov_2016.pdf [https://perma.cc/5U2N-3MD6] (describing a variety of perspectives on the ways in which Australia needs to modernize and solidify its cybersecurity strategy); Nawaf Bitar, *Advanced Cyber Attackers Necessitate an Active Defense*, ABC TECHNOLOGY & GAMES (Aug. 1, 2014), http://www.abc.net.au/technology/articles/2014/08/01/4058780.htm

studies in greater context, hence the following section that unpacks the G7's efforts to regulate active defense.

3.5. G7

Although a deep dive into each G7 nation is beyond the scope of this inquiry and has already been accomplished elsewhere,[136] Table 3 does provide a synopsis of each jurisdiction's current regulation of active defense.

Table 3: Sample of Regulations from G7 Nations Pertaining to Active Defense[137]

[https://perma.cc/9UNC-JT4G] (arguing for Australia to adopt an approach of "Active Defense, which looks to actively disrupt attackers when they are attempting to attack an organization's infrastructures, but without crossing the line and risking retaliation.").

136 *See* Craig, Shackelford & Hiller, *supra* note 11 at 740–743.

137 *Id.* (providing an earlier version of this table). These data were assembled from the following sources: Donna Simmons, *Laws of Canada as they Pertain to Computer Crime*, SANS INST. (2002), https://www.sans.org/reading-room/whitepapers/legal/laws-canada-pertain-computer-crime-673 [https://perma.cc/ZU64-YBXL]; Cybercrime and the *Criminal Code*, CAN. DEP'T JUST. (2012), https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention/cybercrime.html; *France*, CYBERCRIME LAW, http://www.cybercrimelaw.net/France.html [https://perma.cc/88MP-ZJUA]; 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/ [https://perma.cc/TH4C-3KL3]; *Germany*, CYBERCRIME LAW, http://www.cybercrimelaw.net/Germany.html [https://perma.cc/TRJ5-YEV2]; Bettina Weisser, *Cyber Crime – The Information Society and Related Crimes* (2013), http://www.penal.org/spip/IMG/file/RM-8.pdf; *Italy*, CYBERCRIME LAW, http://www.cybercrimelaw.net/Italy.html [https://perma.cc/UP8X-R6Q6]; *Japan*, CYBERCRIME LAW, http://www.cybercrimelaw.net/Japan.html [https://perma.cc/7R8Q-F2C2]; 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/ [https://perma.cc/TS6Y-39MP]; Japanese Cyber Security Strategy and related Documents, http://www.space-cyber.jp/cyber/ [https://perma.cc/5S62-SHWW]; Ryusuke Masuoka & Tsutomu Ishino, *Cyber Security in Japan*, CIPPS (2012), http://www.cipps.org/group/cyber_memo/003_121204.pdf [https://perma.cc/8CPV-U6KZ]; Takato Natsui, *Cybercrimes in Japan: Recent Cases, Legislations, Problems and Perspectives*, http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf [https://perma.cc/5492-NWY9]; Robert Lipovsky, Aleksandr Matrosov, & Dmitry

COUNTRY	TITLE OF LAW	YEAR OF LAW	RELEVANT LANGUAGE
Canada	• Criminal Code of Canada § 342.1 • Criminal Code of Canada § 430(1.1)	• 1985 • 1985	• "Every one 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.

Volkov, *Cybercrime in Russia: Trends and Issues*, ESET (2011), https://www.slideshare.net/matrosov/cybercrime-in-russia-trends-and-issues [https://perma.cc/PNE4-JH6A]; 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/ [https://perma.cc/8GAZ-UNLT]; *U.K.*, CYBERCRIME LAW, https://www.cybercrimelaw.net/UK.html [https://perma.cc/4XXN-JSKJ]. For more information on the U.K.'s efforts with regard to active defense, see *Active Cyber Defense*, NAT'L CYBER SEC. CTR., https://www.ncsc.gov.uk/active-cyber-defence [https://perma.cc/YHJ9-KX58].

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."
United Kingdom	Computer Misuse Act	1990 (amended in 2006— Police and	"(1)A person is guilty of an offence if— a. he causes a computer to perform any function with

		Justice Act, Section 35)	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.'[138] • The Computer Fraud and Abuse Act regulates those who "knowingly" or "intentionally" access "a computer without authorization or exceed[] authorized access . . . ." 18 U.S.C. § 1030(a)(2).

[138] For a thorough review of U.S. cybercrime law as it pertains to active defense and "hacking back," see *Prosecuting Computer Crimes*, DEP'T JUST., OFF. LEGAL EDUC., 3, tbl. 1 (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [https://perma.cc/474U-LQH7].

			• 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)."[139]

At least three converging trends are apparent from Table 3, among them: (1) the fact that every G7 nation, as well as all 50 U.S. states along with Thailand, forbids unauthorized access, demonstrating the uphill battle faced by new active defense legislation; (2) that these laws are mostly dated at this point given the fast pace at which cybersecurity is advancing, as well as being rather broad, similar to China and Australia's approaches (Canada's Criminal Code regulates unauthorized access broadly as "[e]veryone [who] commits mischief"[140]); and (3) that the penalties involved vary greatly. Fines can reach 30,000 euro in France.[141] The duration of jail time, though, does show more consistency, with the exception of the United States, where sentences can exceed 20 years

---

139 *Id.* at 5.

140 Criminal Code, R.S.C. 1985, c C-46, § 430(1.1) (Can.).

141 CODE PÉNAL [C. PÉN.] [PENAL CODE] art. 323-1 (Fr.); UGOLOVNIY KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 272 (Illegal Accessing of Computer Information) (Russ.). One area of divergence between these nations involves the cybersecurity requirements on protected systems before the legal regime is activated. In both Germany and Italy, for example, only networks "specially protected against unauthorized access" are covered. STRAFGESETZBUCH [STGB] [PENAL CODE], § 202(a) (Data Espionage), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [https://perma.cc/T8YY-YT6D] (Ger.); Penal Code art. 615-ter. (Unauthorized access into a computer or telecommunication system) (It.).

for CFAA violations. [142] Political convergence across the G7, facilitated in no small part by the Council of Europe Convention on Cybercrime (Budapest Convention), [143] has also helped propel common cybersecurity norm building across this group. For example, in 2017 the G7 reiterated a list of non-binding cybersecurity norms, which were first identified in the 2015 United Nations Group of Governmental Experts report and G20 Leaders' Communiqué,[144] a topic returned to in Part IV.

---

[142] *Prosecuting Computer Crimes*, DEP'T JUST., OFF. LEGAL EDUC. 3, tbl. 1 (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [https://perma.cc/474U-LQH7].

[143] Convention on Cybercrime, Council of Europe, E.T.S. 185 (Nov. 23, 2001), http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm [https://perma.cc/84EJ-FSBQ] [hereinafter Cybercrime Convention]. *See also* Stein Schjolberg, *The History of Global Harmonization on Cybercrime – The Road to Geneva*, CYBERCRIME LAW, at 3, (Dec. 2008), http://www.cybercrimelaw.net/documents/cybercrime_history.pdf [https://perma.cc/DKL2-5ZTE] (discussing the history of G8 efforts to mitigate cybercrime).

[144] Group of Seven, *G7 Declaration on Responsible States Behavior in Cyberspace*, at 3–5 (Apr. 11, 2017), https://www.mofa.go.jp/files/000246367.pdf [https://perma.cc/RVU9-YA5V] ("1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security; 2. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences; 3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; 4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect; 5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression; 6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public; 7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions; 8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory,

4. IMPLICATIONS FOR MANAGERS AND POLICYMAKERS

This final part explores some of the myriad implications of permitting particularly more aggressive active defense measures as a matter of policy, beginning with the underappreciated intersection of proactive cybersecurity and cyber risk insurance. Next, we move on to possible reform efforts, before concluding with a wider discussion about the place of active defense as part of a push toward cyber peace.

4.1. Cyber Risk Insurance

Insurance has long been recognized as being an important tool in mitigating cyber risk, but is one that is relatively immature and "not standardized, likely resulting in coverage gaps and a litigious claims environment."[145] After all, insurance is a risk management mechanism across sectors ranging from automobiles to floods. Realizing the market opportunity, insurance firms have been experimenting with cyber risk insurance policies since the early

---

taking into account due regard for sovereignty; 9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; 10. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure; 11. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity. 12. No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.").

145 W. Jean Kwon, The Insurance Business in Transition to the Physical-Cyber Market: Communication, Coordination and Harmonization of Cyber Risk Coverages, SSRN WORKING PAPER (June 28, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201875.

2000s.[146] The market might exceed $7.5 billion by 2020,[147] a trend that is being fueled by new regulatory requirements such as Europe's General Data Protection Regulation (GDPR).[148]

Yet, active defense is an arena that is only beginning to be considered by insurance professionals. According to Stephen Vina, a senior vice president at Marsh Insurance:

> The cyber insurance market can adjust rather quickly to new and evolving threats and cybersecurity techniques, but active defense injects a level of legal uncertainty and risk that carriers are unlikely to embrace at this time. However, there is a wide range of active defense techniques and carriers will undoubtedly work with their clients during the underwriting process to ensure they fully understand the practices involved, risks posed, and legality of the activity. Should active defense gain firmer legal footing, some in the cyber insurance industry may find it advantageous to develop creative risk transfer solutions that can help provide companies some financial protection as they look to better secure their networks with more advanced techniques. Moreover, cybersecurity companies may look to the insurance industry to provide coverage for

---

146 Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm [https://perma.cc/3P6E-38BF]; *see also Safeonline Launches Internet Security Insurance*, HISCOX, https://www.cc.gatech.edu/computing/acmnews/msg00349.html.

147 *See* Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*, REUTERS (Oct. 12, 2015), http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012 [https://perma.cc/HYM6-EXJY]; Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES (Dec. 29, 2011), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ [https://perma.cc/5EBR-3LKE]; Robert Lemos, *Should SMBs Invest in Cyber Risk Insurance?*, DARK READING (Sept. 9, 2010), https://www.darkreading.com/should-smbs-invest-in-cyber-riskinsurance/d/d-id/1134322?piddl_msgorder=thrd [https://perma.cc/47SV-RSBL].

148 *See* Carolyn Cohn, *Europe's New Data Privacy Law Boosts Cyber Insurance Sales*, INS. J. (May 22, 2018), https://www.insurancejournal.com/news/international/2018/05/22/489977.htm [https://perma.cc/XZ2V-E5WU] ("Insurers say the directive, together with major cyber attacks like last year's WannaCry and NotPetya viruses, is driving demand in Europe for cyber insurance—a sector seen as relatively profitable.").

> potential liability stemming from their active defense services.[149]

It is likely that, regardless of new federal and state regulations, the insurance industry will have an important role in shaping corporate proactive cybersecurity policies, especially if a critical mass of insurance providers elect not to insure companies that engage in hacking back. That being said, activities that fall more on the passive side of the active defense spectrum outlined in Figure 1 (e.g., intelligence gathering, intrusion reporting, honeypots, etc.) are already becoming mainstays of effective cybersecurity risk management,[150] and as such may be encouraged by insurers.

4.2. Reform Efforts

Continuing confusion over the scope and meaning of the CFAA specifically, and the permissible bounds of active defense in the United States and abroad generally, has led to efforts aimed at ensuring greater clarity. In the United States this stems from potential policy reforms through both the executive and legislative branches. For example, a 2016 George Washington University report called on the Executive to:

> 1. [I]ssue public guidance to the private sector with respect to active defense measures that it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company's own information and systems. Such guidance should be updated on a regular basis consistent with ongoing developments in technology.
>
> 2. DOJ and the Federal Trade Commission should update their "Antitrust Policy Statement on Cybersecurity Information Sharing" (2014) to state clearly that antitrust

---

149 Interview with Stephen Vina, Senior Vice President, Marsh Insurance, in New York, NY (July 10, 2018).

150 *See, e.g.*, Mark Dargin, *Increase Your Network Security: Deploy a Honeypot*, NETWORK WORLD (Oct. 24, 2017), https://www.networkworld.com/article/3234692/lan-wan/increase-your-network-security-deploy-a-honeypot.html [https://perma.cc/6FV9-68R7] (providing a useful description of the term "honeypot").

> laws should not pose a barrier to intra-industry coordination on active defense against cyber threats.
>
> 3. The Department of Homeland Security should coordinate the development of operational procedures for public-private sector coordination on active defense measures, utilizing existing mechanisms for cooperation such as the industry-led Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), and the National Cybersecurity and Communications Integration Center (NCCIC) at DHS.[151]

The report, which included a number of notable co-chairs including the former Secretary of Homeland Security Michael Chertoff, also suggested that NIST develop best practices with regard to active defense (building from its work on the CSF), that federal agencies fund new active defense research and development initiatives, that the State Department work with international partners on active defense norms development, and that the White House work to define what steps federal agencies may take on helping the private sector with active defense measures and with coordinating this effort.[152] Many of these steps, though, will be difficult to take under the Trump Administration's current policies, given U.S. disengagement from numerous multilateral fora including in the Internet governance space.[153]

What can, or should, Congress do to help rethink active defense? The George Washington Report suggests that Congress should pass legislation to oversee the Executive Branch efforts outlined above, but it also calls on Congress to amend the CFAA "to ensure that low- and medium-risk active defense measures are not directly prohibited in statute."[154] However, what is meant exactly by "low- and medium-risk" measures is left undefined in the Report, a somewhat curious omission given the well-known difficulties of attribution and escalation in this space. This suggestion, though, would seem to include a reformed Graves bill, so long as the legislation incorporated appropriate (and mandatory) oversight,

---

151 INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS, CTR. FOR CYBER & HOMELAND SEC., at xii–xiii (2016), https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf [https://perma.cc/8P8K-QTBT].

152 *Id.* at xiv.

153 *See* Osnos, *supra* note 105 (suggesting the U.S.'s disengagement).

154 INTO THE GRAY ZONE, *supra* note 151, at xiii.

clarified which types of primarily passive active defense such as beaconing are permissible under other federal laws besides CFAA,[155] clarified the scope and key terms used such as what is meant by "persistent" breaches and "*computer* of the attacker,"[156] and was limited to only a narrow subset of the most damaging cyber attacks, perhaps those targeting critical infrastructure sectors such as the power grid, water, transportation, healthcare, and banking. A pilot program, perhaps building from Singapore's experience, would help in this regard given ongoing concerns over attribution and the numerous other objections to *aggressive* active defense discussed above.

Finally, to establish industry active defense best practices, the private sector can, and should, create new fora to coordinate responses between stakeholders including Internet and Cloud service providers, and leverage corporate governance to wargame various scenarios and think through responses.[157] The insurance industry can be a partner in this undertaking, as can other global stakeholders. For example, Siemens unveiled its "Charter of Trust" during the 2017 Munich Security Conference, which listed ten norms "to enhance confidence in technology[,] including: "supply-chain protection," "security by default," and "innovation," which includes deeper public-private partnerships that could include active defense.[158] When combined with Microsoft's push for a Digital Geneva Convention, which would aim to, among other things, protect critical infrastructure while limiting the development and use of cyber weapons,[159] there seems to be a growing appetite for active private-sector engagement in cybersecurity norm building. In

---

155 *See* Chris Cook, *Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act*, JUST SECURITY (Nov. 20, 2017), https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/ [https://perma.cc/DJR5-WPUP] (noting that the proposed ACDC Act "only amends the CFAA and says nothing about the electronic surveillance statutes such as the Wiretap Act, the Electronic Communications Privacy Act, and the Pen Register Trap and Trace statute."). Beaconing is the "the continuous transmission of small packets (beacons) that advertise the presence of the base station." *Beaconing*, PC MAG. ENCYCLOPEDIA, https://www.pcmag.com/encyclopedia/term/38503/beaconing [https://perma.cc/PZ44-G97J].

156 *Id.*

157 *Id.* at xiv.

158 Garrett Hinck, *Private Sector Cyber-Norm Initiatives: A Summary*, LAWFARE (June 25, 2018), https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary [https://perma.cc/54QZ-M8V9].

159 *Id.*

fact, in April 2018, thirty-four leading tech firms—including Microsoft and Facebook—signed the "Cybersecurity Tech Accord," which calls on signatories to help safeguard "users and customers" from cyber attacks, and "oppose attacks on civilians and businesses," which, it seems, includes a prohibition on hacking back.[160] Such partnerships, including the Paris Call discussed next, while not being embraced by all nations as of this writing, are also indicative of a shift toward a more polycentric approach at enhancing global cybersecurity in what could be considered a push for cyber peace.

4.3. Prospects for a Proactive Cyber Peace

"Cyber peace" has been defined by the U.N. as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence."[161] However desirable, such a cyber end-game is unlikely, at least in the near term.[162] Cyber peace is defined here, as it has been done in previous works, not as the absence of conflict or what may be called negative cyber peace.[163] Rather, cyber peace is:

> the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure

---

160 *Id.*; CYBERSECURITY TECH ACCORD, https://cybertechaccord.org/accord/ [https://perma.cc/ER8R-MUCS].

161 Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [https://perma.cc/7CLB-KY5R] (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace").

162 *Cf.* at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients").

163 The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957) (arguing "[t]rue peace is not merely the absence of some negative force—tension, confusion or war; it is the presence of some positive force—justice, good will and brotherhood").

> systems, and couches cybersecurity within the larger debate on Internet governance. [164]

Working together through polycentric partnerships—such as those Cybersecurity Tech Accord and Siemens's Charter of Trust discussed above—"we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration."[165] A key aspect of that effort is engaging in dialogue, including about key policy differences surrounding cyber sovereignty, [166] lest the worrying trend toward Internet fragmentation continue unabated.[167]

What role can active defense play in such an undertaking? Critics abound. Some commentators, for example, make the case that deterrence-by-denial should be at the forefront of cybersecurity policy given "[p]roblems of attribution, displays of power, controllability and the credibility of digital capabilities." [168] According to Professor Patrick Lin:

> It is much too premature to allow for hacking back, even if the practice isn't immoral . . . At minimum, there needs to be a clear process to authorize or post-hoc review cyber counterattacks to ensure they're justified, including penalties

---

164 SHACKELFORD, *supra* note 23, at xxv.

165 Id.

166 *See* Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. The Multistakeholder Model*, BELFER CTR. (Aug. 2019), https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=China_Cyber_Sovereignty_paper%20(2)&utm_content=&spMailingID=21986839&spUserID=MjMwNjM5MzgzMTQ0S0&spJobID=1561316105&spReportId=MTU2MTMxNjEwNQS2 ("The divide between nations that support governance models based on cyber sovereignty, primarily China and Russia, and those that believe in the multi-stakeholder model, including most liberal democracies, is one of the most prominent ideological conflicts dividing cyberspace. Enhancing understanding on both sides of these philosophies is an important step toward preventing further fragmentation of cyberspace and necessary for avoiding conflict.").

167 Daniel Voelsen, *Cracks in the Internet's Foundation: The Future of the Internet's Infrastructure and Global Internet Governance*, SWP RESEARCH PAPER, at 1 (Nov. 2019), https://www.swp-berlin.org/en/publication/cracks-in-the-internets-foundation/.

168 Matthias Schulze, Cyber Deterrence is Overrated, SWP Comment No. 34, at 1 (Aug. 2019), https://www.swp-berlin.org/fileadmin/contents/products/comments/2019C34_she.pdf.

> for irresponsible attacks. That oversight infrastructure hasn't even been sketched out.[169]

The ACDC Act is an attempt at mitigating Professor Lin's concerns by tapping the FBI to play an oversight role. But this still does not get to the bigger issue. As was argued in the *New Yorker*, "[s]hould hacking back become legal, it may well help individual victims of cybercrime, but it is unlikely to make the Internet a safer place."[170] This view is shared by Chris Cook of the U.S. Department of Justice, who said "the crucial question policymakers should be asking is whether we are comfortable allowing foreign actors/private entities to do on our own networks what we are proposing to authorize on theirs."[171] Such a destabilizing development would curtail efforts aimed at establishing international cybersecurity norms, as James Lewis, among others, has argued, potentially leading to "an abandonment of U.S. efforts to establish international norms against this type of activity."[172] Concerns over friendly fire, and firms being caught in the middle of protracted cyber conflicts involving myriad private- and public-sector stakeholders, did little to convince the Trump Administration, for example, to embrace the Paris Call for Trust and Stability in Cyberspace. This agreement is a multi-stakeholder statement of principles designed to help guide the international community toward greater cyber stability, and perhaps one day cyber (also known as digital) peace. In particular, the agreement calls for action to safeguard civilian infrastructure, Internet access, and for the international community to "[t]ake steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors."[173] On the day it was announced, more than 50 nations (with the notable exception of the United States), "130 companies and 90 universities and nongovernmental groups" signed the Paris Call,[174] including its pledge against allowing for aggressive active defense.

---

169 Wolff, *supra* note 2.

170 Schmidle, *supra* note 33.

171 Cook, *supra* note 155.

172 *Id.*

173 PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE (Nov. 12, 2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf [https://perma.cc/79JX-2LZE].

174 David E. Sanger, *U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks*, N.Y. TIMES (Nov. 12, 2018),

This emerging international norm against aggressive active defense does not mean, though, that proactive cybersecurity—especially on the *passive* side of the active defense spectrum—is not essential to building resilience and due diligence across vulnerable critical infrastructure sectors. In fact, such a "lean in" approach to cybersecurity is essential to help guard against the more reactive mindset that has long bedeviled the field of cybersecurity risk management.[175] And more firms seem to be embracing this viewpoint, even as there is continued strong resistance from the tech community as seen in the Cybersecurity Tech Accord, across the G7, and in all 50 U.S. states. According to Vina:

> Legal uncertainties and potential unintended consequences currently limit the practicality of active defense, leading to more risk than reward at this point in time. When viewed across a comprehensive cybersecurity risk management strategy, firms are more inclined to select better established cyber defenses with identifiable metrics that meet business, contractual, or regulatory requirements. That said, interest in active defense appears to be slowly growing as policy makers consider cyber legislation to address more sophisticated threats and cybersecurity within the business community matures, leaving the door open for this tool to grow in importance in the coming years.[176]

As the political winds shift, and more firms suffer from cyber attacks that governments have so far failed to stop, *passive* active defense may well become more mainstream in more nations. The question is one of institutional clarify, harnessing the benefits while minimizing the myriad risks in this practice.[177] Already, in 2019 the

---

https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html [https://perma.cc/UD5N-VCTN]; *Indiana University Among First to Endorse Paris Call for Trust and Security in Cyberspace*, IU NEWSROOM (Nov. 12, 2018), https://news.iu.edu/stories/2018/11/iu/releases/12-paris-call-for-trust-and-security-in-cyberspace.html [https://perma.cc/X9KZ-UVFH].

175 MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [https://perma.cc/N6L4-KAML] (comparing cybersecurity investment rates across countries and concluding that "it appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive").

176 Vina, *supra* note 149.

177 *See* Dalibor Rohac, *Indiana's Gift to the International Order*, AM. INTEREST (May 10, 2018), https://www.the-american-interest.com/2018/05/10/indianas-

United States along with twenty-six other nations issued a "Joint Statement on Advancing Responsible State Behavior in Cyberspace," which underscored the point that "the international rules-based order should guide state behavior in cyberspace.[178] Yet this Statement also maintained that these nations would "work together on a voluntary basis to hold states accountable when they act contrary" to the goal of ensuring "a free, open, and secure cyberspace for future generations."[179] Clearly, then, "responsible" State behavior remains in the eye of the beholder with accountability mechanisms polycentric in nature, and still rather nascent. Such a deficit in cybersecurity governance calls out for active engagement.

5. CONCLUSION

This Article has tracked the debate surrounding active defense, detailing how the policy has evolved at the state and federal level in the United States, across the G7, and in other major economics, including China, Australia, Thailand, and Singapore. Across these jurisdictions, we see a historic reluctance to embrace the notion of aggressive active defense (e.g., hacking back), and instead there has been a marked trend toward criminalizing unauthorized access. However, the Georgia hack-back bill, the ACDC Act, and Singapore's active defense policies portend policy shifts in the making that could destabilize the status quo and impact on cybersecurity norm developments. At a time when many forums are being created and repurposed to promote stability, and even some measure of cyber peace, if more nations permit active defense then this progress, in the form of nascent norms as embodied in the Paris Call, could be scuttled. To avoid this outcome, any policy of permitting active defense should be narrowly tailored to only allow passive active defense measures under strict government oversight, and only then for the worst cyber attacks on civilian critical infrastructure sectors. A better option might be to pursue an attribution council that would allow for unbiased, third party

---

gift-to-the-international-order/ [https://perma.cc/3AJT-ZDAB] (suggesting the need for balance between risks and benefits).

178 JOINT STATEMENT ON ADVANCING RESPONSIBLE STATE BEHAVIOR IN CYBERSPACE, U.S. DEP'T ST. (Sept. 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

179 *Id.*

investigations of cyber attacks without assignment of liability.[180] Ultimately, we should embrace the best of proactive cybersecurity while not letting the quest for cyber peace degenerate into a tit-for-tat battle of digital vigilantes seeking to protect their networks but ultimately exacerbating the very cyber insecurity they are fighting to end.

---

[180] *See, e.g.*, Karl Grindal et al., *Institutionalizing Transnational Cyber Attribution: A Survey and Research Agenda* (Ostrom Workshop Working Paper, 2018), https://ostromworkshop.indiana.edu/pdf/seriespapers/2018fall-colloq/mueller-paper.pdf (providing a proposal of an attribution council).

* * * * * *