REPORT DOCUMENTATION PAGE	*Form Approved* **OMB No. 0704-0188**

1. REPORT DATE *(DD-MM-YYYY)* 05/23/2019	**2. REPORT TYPE** Masters thesis	**3. DATES COVERED** *(From - To)* Sep 2018 - May 2019

4. TITLE AND SUBTITLE A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Corcoran, Brian, D.	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Civilian Institutions Office (Code 522) Naval Postgraduate School 1 University Circle, Herrmann Hall Rm HE046 Monterey, CA 93943-5033	**10. SPONSOR/MONITOR'S ACRONYM(S)** NPS CIVINS **11. SPONSORING/MONITORING AGENCY REPORT NUMBER**

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The U.S. private sector is under attack in cyberspace. An increasingly mainstream national security argument calls for amending U.S. law to permit private sector actors, either by themselves or under government supervision, to take so-called “active defense” measures—technical measures that fall in the grey zone between passive network defenses and aggressive offense. This essay identifies and surveys the relevant laws of twenty countries with large and technologically innovative private sectors. As the U.S. government considers how best to protect U.S. private industry, this "map" informs the options on the table for a holistic review and response to the problem.

15. SUBJECT TERMS

Cybersecurity, active defense, cyber laws, private sector, international law, Budapest Convention on Cybercrime, Computer Fraud and Abuse Act (CFAA), self-defense, cyberspace

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	70	**19b. TELEPONE NUMBER (*Include area code)***

THIS PAGE INTENTIONALLY LEFT BLANK

A COMPARATIVE STUDY OF DOMESTIC LAWS CONSTRAINING PRIVATE SECTOR ACTIVE DEFENSE MEASURES IN CYBERSPACE

Brian Corcoran[1]

LL.M. Program, 50-page paper

Submitted: May 2019

Supervisor: Jack Goldsmith

[1] Lieutenant Commander, Judge Advocate General's Corps, U.S. Navy. LL.M. candidate, 2019, Harvard Law School; J.D., 2009, Geo. Univ. Law Center (cum laude); A.B., 2006, Brown Univ. (magna cum laude). Member of the bar of Pennsylvania. The views expressed here are mine and do not reflect the official policy or position of the Department of the Navy, Department of Defense, or the U.S. Government. Research paper submitted in partial fulfillment of the requirements of a Master of Laws (LL.M.) degree at Harvard Law School.

ABSTRACT

The U.S. private sector is under attack in cyberspace. An increasingly mainstream national security argument calls for amending U.S. law to permit private sector actors to take so-called "active defense" measures—technical measures that fall in the grey zone between passive network defenses and aggressive offense. Private sector use of active defense measures such as "honeypots," "sinkholes," "beacons," or "tracebacks" can slow, identify, or even deter offenders in cyberspace, provide unclassified evidence for use in civil cases, or support a government response. The risk is that additional careless or incompetent actors in cyberspace could create more problems than they could possibly help solve.

Many of the questions debated in the U.S. conversation around private sector active defense—in particular, whether U.S. actors are too constrained or not constrained enough—would clearly benefit from comparison to other states' domestic laws. What are other ways of doing things? What laws apply, and where? To date there has been no systematic effort to map out the cyberspace terrain across jurisdictions. This essay identifies and surveys the relevant laws of twenty countries with large and technologically innovative private sectors. It concludes that even if Congress relaxes U.S. law explicitly to permit certain private sector active defense measures, as has been contemplated, laws around the world will continue to constrain private sector activity.

TABLE OF CONTENTS

I. Background

a. Framing the Situation

In November 2017, General (retired) Keith Alexander, the former United States (U.S.) National Security Agency (NSA) director, warned a group of journalists, "You can't have companies starting a war."[2] One year later, Microsoft President Brad Smith told an assembly of technologists, "When we are talking about cyberspace, fundamentally we are talking about space that is private property, we're talking about datacenters and undersea cables and laptops and phones and devices and services that we create. Like it or not, and I don't think we should like it, the reality is inescapable; we have become the battlefield."[3]

The United States, for all its vast public sector national security resources, has long wrestled with how best to counter espionage, theft, and destruction in cyberspace. The "battlefield" metaphor got a jolt in 2017 when back-to-back episodes of state-linked cyber activity shut down hospitals in the United Kingdom (U.K.), Slovakia, and Indonesia; universities in China, Canada, and Italy; police stations, courts, and local governments in India, Brazil, and Sweden; ministries in Russia and Romania; telecom companies in Portugal, Spain, and South Africa; multinationals including Boeing, Honda, Hitachi, Petrobras, and FedEx; law firms; oil companies; ports; the radiation monitoring system at Chernobyl; and one fifth of all global shipping—among many other victims.[4]

[2] Lorenzo Franceschi-Bicchierai, *Ex-NSA Director Says Companies Should Never Hack Back Because They Could Start Wars*, VICE, Nov. 6, 2017, https://perma.cc/3JZJ-FPA9 (quoting Alexander's address to the CyberConnect 2017 conference in New York City).

[3] Steve Ranger, *Why Microsoft is fighting to stop a cyber world war*, ZDNET, Dec. 12, 2018, https://perma.cc/XKH2-UEVV (quoting Smith's remarks to the November 2018 Web Summit conference in Lisbon).

[4] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED, Aug. 22, 2018, https://perma.cc/9F2J-4UC7; *see also*, *e.g.*, Agamoni Ghosh & India Ashok,

As of 2019, the number of known or suspected state-linked cyber activities both systematically and incidentally targeting private individuals and corporations continues to grow.[5] Today, attackers in cyberspace have an undisputed asymmetric advantage over defenders.

What can and should a private actor do in the face of this "inescapable" reality? International law and norms provide little if any guidance. As far as we know, inter-state cyber conflict and ensuing cyber damage has so far stayed below the "use of force" and "armed attack" thresholds in the United Nations Charter.[6] Few states have yet responded to cyberattacks on their private sector with real-world lethal force, although some appear to have considered or responded with cyber countermeasures.[7] Historically, the United States with its massive but vulnerable private sector has feared escalating counter-retaliation and in any case cannot defend everywhere at all times both because of

WannaCry: List of major companies and networks hit by ransomware around the globe, INT'L BUS. TIMES, May 16, 2017, https://perma.cc/9YUK-K2ZF.

[5] The Council on Foreign Relations maintains a database of the publicly known (or publicly-believed-to-be) state-sponsored incidents since 2005 at https://perma.cc/CC5C-X9P8. *See also* Aimee O'Driscoll, *100+ Terrifying Cybercrime and Cybersecurity Statistics and Trends, 2018 edition*, COMPARITECH, Oct. 2, 2018, https://perma.cc/5ETV-L4SD (compiling studies on the prevalence of cyber threats) and Dan Simmons, *Cyber-attacks 'damage' national infrastructure*, BBC NEWS, Apr. 5, 2019, https://perma.cc/GJX7-UKZ5 (polling of critical infrastructure IT personnel indicating 90% have been hacked).

[6] U.N. Charter arts. 2(4) & 51. *See also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt, ed., 2017), https://doi.org/10.1017/9781316822524 ("States have to deal with cyber issues that lie below the use of force threshold on a daily basis."). Although Schmitt and others have concluded elsewhere that Stuxnet likely met the "use of force" threshold, Iran did not make that claim in any international body. Similarly, Estonia ultimately did not claim that the 2007 DDoS attack was an "armed attack" triggering NATO Article 5. *See* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED, Aug. 21, 2007, https://perma.cc/N2SZ-SJTZ.

[7] For the theory of countermeasures in cyberspace generally, *see* Michael Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014); *see also* Matthew Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1 (2009). Several states have either asserted or employed the right to respond to cyberattacks *within an ongoing armed conflict* with lethal force. *See, e.g.*, the Israel Defense Forces strike of May 5, 2019, https://perma.cc/RA5W-R8TF. *But see* Ryan Maness, *The Dyadic Cyber Incident and Dispute Data, Version 1.1*, https://perma.cc/U2DY-4KT5 (U.S. Naval Postgraduate School study cautioning that, contrary to popular perception, relatively few known state conflicts through 2014 have so far involved a (known) cyber component. The study is scheduled to be updated in May 2019 with data through 2016).

resource constraints and still-strong domestic norms.[8] Although in 2019 the United States and allied governments are said to be pursuing state policies of "active defense" and "defend forward" postures in cyberspace, it is hard in an unclassified public setting to know how, how much, and how fast. [9]

In the face of apparent government inaction or inefficacy today, so the story goes, some of the world's vast and technologically savvy transnational corporations and non-governmental organizations want to "hack back" or to employ so-called "active defense" measures.[10]

[8] *See generally* Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*, HOOVER WORKING GROUP ON NAT. SEC. TECH. & L., Aegis Series Paper No. 1806 (Jun. 5, 2018), https://perma.cc/L8S9-X2AY.

[9] *See, e.g.*, recent announcements by NATO (*e.g.*, Robin Emmott, *NATO mulls 'offensive defence' with cyber warfare rules*, REUTERS, Nov. 30, 2017, https://perma.cc/6T5W-V6NR), the U.S. (*National Cyber Strategy of the United States of America*, Sep. 2018, https://perma.cc/5C9H-JU4U), the U.K. (*National Cyber Security Strategy 2016 to 2021*, Nov. 1, 2016, updated Sep 11, 2017, https://perma.cc/3967-GFHM), France (*see* Arthur P. B. Laudrain, *France's New Offensive Cyber Doctrine*, LAWFARE, Feb. 26, 2019, https://perma.cc/YD8N-AQUT), and Germany (*see* Nele Achten, *Germany's Position on International Law in Cyberspace*, LAWFARE, Oct. 2, 2018, https://perma.cc/S2DY-9Z98). The term "active defense" emerged out of military doctrine, as a term referring to "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, http://www.jcs.mil/Doctrine/DOD-Terminology/.

[10] For the key U.S. legal debates, *see* Orin Kerr, Eugene Volokh, and Stewart Baker, *The Hackback Debate*, STEPTOE CYBERBLOG, Nov. 2, 2012, https://perma.cc/G98R-8HSK. For an excellent history of the private sector active defense discussion, *see* Sean Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12 (2014) http://jolt.richmond.edu/v20i4/article12.pdf. For a widely-cited overview of ethical and policy considerations, *see* Patrick Lin, *Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies*, Sep. 26, 2016, https://perma.cc/K57P-4PRV. To illustrate that private industry is seriously contemplating these measures, legal articles, news stories, and think tank reports alike commonly cite a poll of 181 attendees at the Black Hat USA 2012 conference, where over a third stated that they had "engaged in retaliatory hacking" at least once. *See* Brian Prince, *Black Hat Survey: More than 1/3 Have Engaged in Retaliatory Hacking*, SECURITY WEEK, Jul. 26, 2012, https://perma.cc/K9RM-FL4Q. To this we should add that at the 2019 RSA Conference, a poll of 500 attendees found that 72% felt that nation-states should have the right to "hack back" and 58% felt that private organizations have (or should have—the poll phrasing is unclear) the same right. *See* Eva Hanscom, *As the Cyber War Grows, is it Time to Strike Back?*, VENAFI BLOG, March 19, 2019, https://perma.cc/5DL7-N7YN. Without access to the underlying data, it's hard to assess the accuracy of such informal polls; here, I cite them solely for their part in the ongoing "cyberwar" narrative.

b. Terminology—What is "Active Defense"?

In this paper, I use the term "active defense" to mean those technical[11] measures in cyberspace[12] that fall between passive in-network defense (e.g., firewalls, antivirus, security patch management, internal logging, scanning, and monitoring, etc.) and aggressive out-of-network offense (e.g., hacking into another computer in order to delete exfiltrated data or disrupt network operations).

I draw this definition[13] from a 2016 report put out by George Washington University's Center for Cyber and Homeland Security (CCHS) Active Defense Task Force, co-chaired by former NSA director Admiral Dennis Blair; former Secretary of the U.S. Department of Homeland Security (DHS) Michael Chertoff; former Special Assistant to the President for Homeland Security Frank Cilluffo; and former DHS Chief Privacy Officer Nuala O'Connor.[14] In summary, the CCHS Report argues that U.S.

[11] In this essay, I do not address other, non-technical policy tools (e.g., sanctions, indictments, trade remedies, etc.), all of which have clear legal pedigrees, along with well-understood benefits and drawbacks.

[12] "Cyber" is a notoriously unclear term. I use it simply to mean "pertaining to the Internet."

[13] For other possible definitions of "active defense," *see, e.g.*, Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT' L. 103 (2014).

[14] Dennis Blair, et al., *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats* CENTER FOR CYBER AND HOMELAND SECURITY (2016), https://perma.cc/WZR3-3NG3 (hereinafter CCHS Report). That report defines active defense more fully as

> a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with "hacking back" and the two should not be used interchangeably."

Some lawyers and technologists have criticized "active defense" proponents as representing a radical position indistinguishable from aggressive "hacking back." *See, e.g.*, Jacqueline Wolff, *When Companies Get Hacked, Should They be Allowed to Hack Back?*, THE ATLANTIC, Jul. 14, 2017, https://perma.cc/HRL2-AW7M (Wolff is a computer security technology professor at RIT and a Harvard Berkman Klein Center affiliate). Individual recommendations from the CCHS Report may well be criticized on the merits (outside the scope of this essay), but overall the report represents the mainstreaming of what was once thought of as a radical approach. Although the CCHS Report Task Force included some members known for supporting an aggressive private sector role in cyberspace (e.g., Stewart Baker), it also policymakers should encourage technologically-advanced private actors to use active defense measures, subject to a policy and legal framework that "confirms government oversight, ensures that privacy and civil liberties are not infringed, and mitigates technical risks."[15] The report also makes recommendations for how the U.S. executive and legislative branches and private industry might support these measures.

The appeal of allowing the private sector to use active defense measures is that they complement government defenses and can be used to slow, identify, or even deter offenders in cyberspace, to provide evidence for use in civil cases, or to support a government response. The risk of encouraging such measures is that careless or incompetent private sector actors in cyberspace may create more problems than they could possibly help solve: either by recklessly or negligently harming adversary (or intermediary) computers or by inviting counterretaliation.

c. Research Problem

The U.S.-based conversation on active defense measures tends to focus inward, with occasional comments indicating that laws in other countries are surely important but largely a mystery. Those stray comments rarely cite specific laws, specific countries, or specific concerns.

For example, one legislative proposal raised in 2017 would have provided U.S. companies with a defense against prosecution when using active defense measures to

included representative members from banks, law firms, technology companies, academia, insurance companies, cybersecurity companies, etc. Nuala O'Connor wrote separately to indicate where the Task Force was not in consensus on a number of issues. Professor Orin Kerr, not a proponent of active defense, served as consultant. *See, e.g.*, Orin Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J. L. ECON. & POL'Y 197 (2005), https://perma.cc/CS49-TG3Y and Kerr's portion of the debate held on the Volokh Conspiracy blog, *supra* note 10. *See also* Bruce Schneier, *Hacking Back*, SCHNEIER ON SECURITY, Feb 13., 2017, https://perma.cc/ZJG8-6H3X, ("I've never been a fan of hacking back…But the [CCHS Report] makes a lot of good points.")

[15] CCHS Report, *supra* note 14, Foreword at v.

establish attribution, disrupt continued unauthorized activity, or monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques, but cautioned that, irrespective of any changes to U.S. law, "Computer defenders should also exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside."[16] It is unclear what to make of such a warning.

Proponents of active defense often imply without citations that other countries' laws are less stringent than the United States' laws[17] while critics and skeptics suggest without citations that all active defense measures are similarly unlawful (or similarly not clearly lawful) in all countries.[18] These vague references confuse rather than advance the conversation. If other countries' domestic laws are indeed important constraints on U.S. private sector behavior, we need a better sense of what those laws say. This is an underdeveloped area of research.[19]

In this essay, I do something very basic: collect in one place a handful of other countries' laws that might limit the private sector's ability to employ active defense

[16] H.R. 4036, 115th Cong. § 2(9) (2017), the draft "Active Cyber Defense Certainty Act," https://perma.cc/CR6Y-NENJ.

[17] *See, e.g.*, Wyatt Hoffman, *The Future of Cyber Defense*, CARNEGIE ENDOWMENT FOR INT'L PEACE, July 17, 2018, https://perma.cc/857Q-9S5R ("We know there's a growing transnational market for these services and companies that operate in more permissive legal environments are driving it." The article doesn't name which environments these might be. Tracing that transnational market is outside the scope of this essay; two starting places include SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014) and Craig, Shackleford, & Hiller, *infra* note 19.

[18] In his 2014 article, *supra* note 13, Paul Rosenzweig cited Germany's "Hacker paragraph" as one known example of another country's relevant domestic law. Since 2014, many articles have duly recited the German law, but few articles have looked for other examples, except as mentioned *infra* note 19.

[19] The CCHS Report, *supra* note 14, includes a few paragraphs of anecdotal notes on active defense norms in the U.K., France, Estonia, and Israel. *See also* Amanda Craig, Scott Shackelford, & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015) (comparing "unauthorized access" regulation across the G8: Canada, France, Germany, Italy, Japan, Russia, U.K., & U.S.) and Scott 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 (2016) (comparing cybersecurity due diligence efforts in the U.S., Germany, and China).

measures, then compare them with each other and with our general understanding of relevant U.S. laws. Mapping out the terrain in this way illustrates, among other things, how domestic laws in many countries have converged to cover much of the same substantive ground, even in the absence of robust international law.[20]

d. Roadmap

In Part II, I describe in non-technical terms how four examples of private sector active defense measures work and explain how each measure may implicate different types of laws, using U.S. law as an example. In Part III, I briefly comment on (the few) international law and norms in cyberspace as they exist today. In Part IV (the bulk of this essay), I compare parallel domestic laws from a number of countries and ask where the differences among the laws are meaningful. In Part V, I draw some very basic conclusions and ask what this means for the future of the U.S. discussion around private sector active defense.

II. WHAT IS PRIVATE SECTOR ACTIVE DEFENSE?

a. Basic Concepts

The dizzying complexity and rate of change in the digital world mask the ways in which computers are still based on simple concepts. In its simplest form, the Internet is two computers, A and B, sending data back and forth through one or more open channels. Generally, A wants to know that B only sees the data A authorizes B to see, and vice

[20] Helpfully, several years ago in support of a 2013 study the United Nations Office on Drugs and Crime (UNODC) began collecting relevant national laws in a database online. United Nations Office on Drugs and Crime (UNODC) Cybercrime Repository, https://sherloc.unodc.org/cld/v3/cybrepo/. For the study itself, *see* UNODC *Comprehensive Study on Cybercrime*, Draft—February 2013, https://perma.cc/CB8V-CYEF (a note in the disclaimer section of the draft report states that it remains subject to editorial changes, but no revised version has been issued). As some laws hosted there are no longer up-to-date and as the database is not exhaustive, I have verified any information found there with a more current source. In the Appendix to this essay, I provide citations to the most recent English text or translation publicly available in 2019.

versa. If B enters A's computer on a simple two-computer network, A can (with enough training and experience) easily watch B's activity. But once A connects to the Internet as a whole, the amount of data coming into A's computer from every open channel is so vast that it is effectively impossible for A (no matter how expert) to watch for B everywhere.

If A wants to ensure that B can't look at, alter, or delete A's data without being detected, A has several active defense options that come up over and over in the U.S. policy discussion.[21] A can create files that lure B to locations where B is more easily monitored (i.e., honeypots) or A can block or redirect all unknown incoming Internet traffic to a separate place for closer monitoring (i.e., sinkholes). If A fears that B will steal A's data, A might implant code in A's files that send alerts back to A if B opens the file (i.e., "beacons"). If A's data is successfully stolen, A might want to follow B's trail through the Internet, looking for clues along the way (i.e., "traceback").

The technical side of active defense boils down to simple ideas like these, but each may be legally problematic for the reasons explained below. The CCHS report provides a fuller spectrum of examples. Before turning to other countries, here I want to examine just these four ideas, explaining in brief and non-technical terms how each measure works and how each measure may implicate different *types* of laws.[22]

[21] *See* CCHS Report, *supra* note 14; *see also* Paul Rosenzweig, Steven Bucci, & David Inserra, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, HERITAGE BACKGROUNDER, May 5, 2017, https://perma.cc/E22C-LWEB.

[22] For more extensive technical explanation of each of these measures than I provide in this more abstracted summary, *see* Harrington, *supra* note 10. Harrington is a lawyer with an advanced technical background in digital forensics. Harrington also delves more deeply into the legal issues around measures not addressed here, such as intelligence gathering in the deep web and dark web.

b. Four Examples of Active Defense Measures

<u>(1) Honeypots</u>

Honeypots are fake files, file structures, and servers that look real but are carefully segmented from a defender's real network. They are designed to attract and monitor intruders without risk to the real network.[23] The honeypot has no authorized users other than its administrators, so any unexpected access to the file or server is easy to monitor—the intruder cannot slip in and out unnoticed.[24]

Honeypots are problematic in jurisdictions that prohibit private sector actors from recording metadata absent a court order. In the U.S., the legal question is unsettled. Incorporating a legal analysis courtesy of Covington and Burling, the CCHS Report concludes that honeypots set without government oversight may run afoul of the U.S. general prohibition on "trap and trace devices."[25] A number of U.S. commentators have made similar comments,[26] with some arguing that current confusion could be resolved by simple (but not forthcoming) interpretive guidance from the U.S. Department of Justice (DoJ).[27] Even those who argue for the minority view that honeypots *don't* violate the

[23] *See* CCHS Report, *supra* note 14.

[24] For a lay summary of different types of honeypots, *see* Greg Martin, *How to Use "Honeypots" to Overcome Cybersecurity Shortcomings*, POWER MAG., Sep. 1, 2014, https://perma.cc/23M5-LV75.

[25] CCHS Report *supra* note 14, Appendix II at 42. The prohibition on pen register and trap and trace (PRTT) devices is found in 18 U.S.C. § 3121. A pen register device records outgoing metadata; a trap and trace device records incoming metadata. Originally drafted for the telephone age, the PRTT prohibition has been read to encompass Internet communications.

[26] *See, e.g.*, Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, STAN. L. & POL'Y REV. 205, 212 (2018), https://perma.cc/6VTR-PRLD; *see also* Rosenzweig, *supra* note 13.

[27] *See* Gregory Falco & Herb Lin, *Active Cyber Defense and Interpreting the Computer Fraud and Abuse Act*, LAWFARE, Dec. 21, 2018, https://perma.cc/73J8-46XX (considering a hypothetical scenario in which an attacker finds a honeypot, begins to exfiltrate data, and the defender corrupts the data packets as they flow out of the system, rather than by "poisoning" the document in advance, Falco and Lin argue that permitting this scenario would be a relatively conservative expansion of current U.S. law, simply by re-interpreting the "knowingly causes transmission" prohibition of 18 U.S.C. § 1030(a)(5)(A) to exclude the defender's modification of its own computing environment).

trap and trace prohibition note that the process of making a realistic fake document may backfire on a company in various ways both practical and legal.[28] As a practical matter, honeypots are widely advertised and employed as cybersecurity measures[29] despite public cautions from the DoJ that the law is "untested."[30]

(2) Sinkholes

The Internet operates, at a very basic level, by dividing data up into small packets, labelling each packet with a numerical address, and sending those packets through a series of routers until all the packets reach their collective destination and can be reassembled into a readable file or executable program. The job of a router is to read the address on each packet and compare it against its routing table, which contains the addresses of each subordinate network in the hierarchy. If the address doesn't appear in the routing table, the router sends (routes) the packet to the next superior router in the hierarchy. On top of this Internet Protocol (IP) hierarchy is overlaid a similar Domain

[28] *See* comments of Robert Clark, now counsel at the Office of the Director of National Intelligence, at the panel discussion *The Ethics of Hacking Back: Cybersecurity and Active Network Defense*, Carnegie Council (Sep. 18, 2013), https://perma.cc/R9HL-4LDW ("Okay, I'm going to set up a honey pot with a bunch of fake documents, deceptions on here. My favorite part of being in New York is the SEC, Security and Exchange Commission. Because what if my documents that are on there are fake mergers and acquisitions with real third parties? If I put crap on there no one's going to steal it, so I've got to make it look real. It gets stolen and then it gets leaked. Now, I didn't disclose it, I didn't put it out there. But when that hits the media, who do you think is going to be knocking on my door? It's going to be the SEC: 'Hey, we're here to investigate you.' 'But that's not mine.' "). Note also that, for U.S. lawyers at least, professional responsibility concerns arise when private sector attorneys are involved in "deceptive" actions. *See* Harrington, *supra* note 10 at 15 and MODEL RULES OF PROF'L CONDUCT R. 8.4(c).

[29] *See, e.g.*, Michael Kassner, *DarkMatter: Curing the internet of digital threats*, TECHREPUBLIC, Aug. 1, 2014, https://perma.cc/WR8U-6NXV (describing U.S.-based Norse Corporation's global network of 8 million honeypots tracking the spread of malware in real time).

[30] William Jackson, *Dangers in luring hackers with honey*, GCN.COM, Aug. 2, 2002, quoting Richard Salgado, then of the DoJ Computer Crime and Intellectual Property Section (CCIPS). The law is still unclear and untested; *see also* the testimony of Richard Salgado, by-then Google's Senior Counsel for Law Enforcement and Security, before the House Judiciary Committee Electronic Communications Privacy Act (ECPA) hearing, Sep. 23, 2010, https://perma.cc/78VR-BNW9, (explaining that the law is full of "complex and baffling rules" in the face of modern challenges).

Name System (DNS) hierarchy, which helps packets find the numerical addresses that are the digital equivalent of "www.google.com."[31]

Sinkholes redirect Internet traffic by providing a false "address" at key points in the hierarchy, which typically requires coordination with the relevant Internet service provider (ISP) or DNS registrar. This is appealing because sinkholes thereby allow defenders to redirect and observe malicious traffic coming into the local network, and perhaps even to disconnect malware-infected computers from the control of malicious actors[32] (so-called "botnet takedowns").[33]

Incorporating a legal analysis from Covington & Burling, the CCHS Report suggests that the U.S. prohibition on "trap and trace" devices may bar active defense measures such as sinkholes that "operate to capture incoming data and identify the source of intrusion or attack."[34] If the sinkhole is deemed to be a trap and trace device, the logical extension is that any U.S. private sector actor who wishes to use sinkholes must work with law enforcement to get a court order.[35] Similarly, the report suggests that practices such as sinkholing may violate the Wiretap Act to the extent that intercepting malicious traffic would be considered an intercept of an electronic communication.[36] Others have noted that, as a practical matter, even if sinkholing without a court order were legal, the ISP or DNS registrar may lack any incentive to help.[37]

[31] For a basic technical overview with helpful diagrams, *see*, *e.g.*, Rus Shuler, *How Does the Internet Work?* (2002), https://perma.cc/S82Z-MRJL.
[32] *See* "What is a DDoS Botnet," CLOUDFARE, https://perma.cc/R7P2-J9JA.
[33] The DoJ, for example, has used sinkholes to take down botnets, starting in 2011. *See* Brian Krebs, *U.S. Government Takes Down Coreflood Botnet*, KREBS ON SECURITY, Apr. 14, 2011, https://perma.cc/BM2C-3FXA.
[34] CCHS Report, *supra* note 14. *See also* 18 U.S.C. § 3121.
[35] For the implications of private sector actors working more closely with law enforcement, *see* comments in Part V, *infra*.
[36] CCHS Report, *supra* note 14 at 42, Appendix II. *See also* 18 U.S.C. § 2510 *et seq.*
[37] *See* Harrington, *supra* note 10 at 17–18.

Of note, the U.S. DoJ advises private actors experiencing cyber intrusions that

> "A system administrator may be able to use a 'sniffer' or other monitoring device to record communications between the intruder and any server that is under attack. Such monitoring is usually permissible, provided that it is done to protect the rights and property of the system under attack, the user specifically consented to such monitoring, or implied consent was obtained from the intruder—e.g., by means of notice or a 'banner.' "[38]

This "stay out of jail by using a banner" advice would seem to give the green light to both honeypots and sinkholes, but legal analysts still routinely use words of uncertainty—"if," "may," and "would"—when trying to assess what legal responsibility might accrue to defenders using such measures. This caution reflects DoJ's more general and oft-quoted proscription for any out-of-network activity:

> "Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as 'hacking back' into the attacker's computer—even if such measures could in theory be characterized as 'defensive.' Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, 'hacking back' can damage the system of another innocent party."[39]

(3) Beacons

Beacons are "[p]ieces of software or links that have been hidden in files and send an alert to defenders if an unauthorized user attempts to remove the file from its home network."[40] Alternately, beacons may be configured to "establish a connection with and send information to a defender with details on the structure and location of the foreign computer systems it traverses"[41]—that is, to "phone home" with details about the route the file has taken and where it currently may be.

[38] U.S. Department of Justice, *Prosecuting Computer Crimes Manual* (2010) [hereinafter DoJ Manual], Appx D at 182, https://perma.cc/5NVA-YHW8.
[39] *Id*. at 180. *See also infra* note 55.
[40] *Id*.
[41] *Id*.

Although beacons may seem harmless and sensible (in that they simply serve as "alarms" for stolen information), by design they may involve unauthorized viewing ("obtaining") of data on another's computer and potentially also execution of a program on another's computer.[42] In the U.S., this is generally seen as violating the 1984 Computer Fraud and Abuse Act (CFAA), which penalizes anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer,[43] [or] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes [any impairment to the integrity or availability of data, a program, a system, or information] without authorization, to a protected computer…"[44]

In a different context, former NSA General Counsel Stewart Baker has argued that if a thief steals data, the owner of the data has implied "authorization" under the CFAA to go retrieve it.[45] The same logic would seem to apply to beacons—that if a thief brings the beacon into its system, any access to information obtained by the use of the beacon would be impliedly "authorized." However, Baker's argument is not generally accepted and, at best, untested.[46] And as is so often the case, the constraints here are

[42] *See also* blog comment by Dave Dittrich (Feb. 14, 2017 at 6:16 pm) on Schneier, *supra* note 14 (Dittrich, a computer security researcher, cautions that beacons neither give "as accurate an attribution as an unsophisticated technical analysis may suggest" and that "someone who doesn't know what they are doing will shoot back at the wrong party.").

[43] 18 U.S.C. §§ 1030(a)(2). "Protected computer" is a term of art including any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). The 7th and 8th Circuits have made clear that all computers connected to the Internet are by definition "used in or affect interstate or foreign commerce or communication" and are thereby protected by the CFAA." United States v. Trotter, 478 F.3d 918 (8th Cir. 2007); United States v. Mitra, 405 F.3d 492 (7th Cir. 2005). *See also* DoJ Manual at 4–5 (summarizing legislative history and noting that even computers not connected to the Internet may meet this definition).

[44] 18 U.S.C. § 1030(a)(5).

[45] *See generally* "The Hackback Debate" between Kerr, Baker, and Volokh, *supra* note 10.

[46] *See, e.g.*, Cook, *supra* note 24 at 212 and the CCHS Report, *supra* note 14 (not coming to a final conclusion on how much legal risk beacon use would incur).

about legal *uncertainty*, not the certainty of prosecution.[47] To resolve some of that uncertainty, in 2017, the "Active Cyber Defense Certainty Act" was introduced in Congress to expressly permit "phone home" beacons; the measure made headlines but never made it out of subcommittee.[48]

(4) Traceback Analysis

Technologically adept companies can sometimes trace a thief's or attacker's trail through the Internet.[49] Note that tracing data through the Internet "means passing through every server the attacker has compromised."[50] As a practical matter, even if the intermediary servers are not harmed, this often means that the tracker is accessing computers without authorization. In the U.S., this generally means the tracker is violating the CFAA.[51]

[47] "Government regulation works by cost and bother, not by hermetic seal." GOLDSMITH & WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD (2006), at 68.

[48] H.R. 4036, 115th Cong. § 3 (2017) would insert the following at the end of 18 U.S.C. § 1030:

"(k) Exception for the use of attributional technology.—

> (1) This section shall not apply with respect to the use of attributional technology in regard to a defender who uses a program, code, or command for attributional purposes that beacons or returns locational or attributional data in response to a cyber intrusion in order to identify the source of an intrusion; if—
>
> (A) the program, code, or command originated on the computer of the defender but is copied or removed by an unauthorized user; and
>
> (B) the program, code or command does not result in the destruction of data or result in an impairment of the essential operating functionality of the attacker's computer system, or intentionally create a backdoor enabling intrusive access into the attacker's computer system.
>
> (2) DEFINITION.—The term 'attributional data' means any digital information such as log files, text strings, time stamps, malware samples, identifiers such as user names and Internet Protocol addresses and metadata or other digital artifacts gathered through forensic analysis."

See also Jacqueline Wolff, *Attack of the Hack Back*, SLATE, October 17, 2017, https://perma.cc/GZS6-CUCX (criticizing the draft Act generally, but calling the beaconing provisions reasonable).

[49] *See generally* Shane Harris, *The Mercenaries*, SLATE, Nov. 12, 2014, https://perma.cc/Z8WN-WGA8 (excerpting from HARRIS, *supra* note 17).

[50] V. Jayaswal, W. Yurcik, & D. Doss, *Internet hack back: counter attacks as self-defense or vigilantism?*, IEEE 2002 INT'L SYMP. ON TECH. & SOC'Y (ISTAS'02), SOC. IMPLICATIONS OF INFO. & COMM. TECH. PROC. (Cat. No.02CH37293), https://ieeexplore.ieee.org/document/1013841 (providing an overview of the technology and terminology of "hack back" as it was in 2002; the commentary is still timely and worth reading to illustrate how little the basic arguments have changed even as the Internet has expanded).

[51] *See* CCHS Report, *supra* note 14 at 14–15.

The most well-known example of a U.S. company "following the trail" is the case of Google's response to "Operation Aurora" in 2009–2010. After Google became aware of a "highly sophisticated and targeted attack on our corporate infrastructure," the company traced the attack back to a server in Taiwan, where Google found information that led it to accuse China.[52] At the time, news reports claimed that Google had entered the Taiwanese server without authorization. Neither Google nor the U.S. government have confirmed or denied this point publicly, but Shane Harris has quoted one "former senior intelligence official who's familiar with the company's response" as saying flatly that "Google broke in to the server."[53] As a practical matter, the authors of the CCHS Report and other informed commentators commonly assume for purposes of discussion that Google likely did enter the Taiwanese server without authorization, which if true almost certainly violated the CFAA.[54] The CCHS Report notes that, "To date, the government has not prosecuted a single company for engaging in active defense measures similar to Google's, although it does warn others of its authority to do so."[55]

In another example of a more "offensive" traceback operation, in 2015 Israeli security firm Check Point[56] accessed the phishing and command-and-control servers of

[52] David Drummond, Google Senior Vice President for Corporate Development and Chief Legal Officer, *A New Approach to China*, GOOGLE OFFICIAL BLOG, Jan. 12, 2010, https://perma.cc/2T8Y-2QPL.
[53] HARRIS, *supra* note 17, chapter 11, "The Corporate Counterstrike," at 172. I assume that quotes provided by established national security journalists like Harris are precise and that the words describing the source should be presumed accurate. For that rule generally (albeit in a different context), *c.f.* Benjamin Wittes, *How to Read a News Story About an Investigation: Eight Tips on Who is Saying What*, LAWFARE, Sep. 4, 2017, https://perma.cc/2VE7-PMBQ.
[54] *See* CCHS Report, *supra* note 14 at 14–15 & 40, Appendix I: Additional Views of Nuala O'Connor. To date, I have not found any U.S. analysis of the episode that makes reference to the corollary Taiwanese prohibition on unauthorized access: Zhōnghuá mínguó xíngfǎ (中華民國刑法) [Criminal Code of the Republic of China] 1935, art. 358 (Taiwan).
[55] CCHS Report, *supra* note 14 at 14 (citing language from a DoJ Computer Crime & Intellectual Property Section (CCIPS) white paper, *Best Practices for Victim Response and Reporting of Cyber Incidents*, Apr. 29, 2015, https://perma.cc/QG52-MN9P, which updates (without changing the substance) the 2010 language cited *supra* note 39.
[56] A NASDAQ 100 company, with offices in the U.S., Canada, Sweden, and Belarus.

the "Rocket Kitten" group (allegedly linked to Iran), thereby identifying both victims and a number of alleged perpetrators. Their public report of investigation demonstrates in an unclassified setting what investigative measures may be technically possible. [57] But many security professionals (not just lawyers) immediately raised concerns about whether that access had been lawful, especially given uncertainties within the report about where the data was physically located.[58] The episode illustrates the fine legal line that those conducting private intelligence analysis walk and sometimes may cross over.

c. In Summary

The technical side of active defense boils down to ideas like these, all of which can be legally problematic in the U.S. for the reasons explained above. Sinkholes protect by interrupting the normal flow of Internet communication. Both honeypots and sinkholes may involve the unlawful collection of metadata absent required oversight. Beacons can run afoul of laws prohibiting access to another's computer and executing code (i.e., reading and writing [altering] data) on another's computer. Traceback missions will almost certainly violate laws prohibiting accessing data on another's computer and can easily turn "offensive."

Assuming the U.S. private sector wants to embrace these legal risks and pursue active defense operations—which will inevitably involve computers both in the U.S. and globally—one reasonable but generally unasked question is: what does the rest of the world think about these types of measures?

[57] *See* Check Point Software Technologies, *Rocket Kitten: A Campaign with 9 Lives*, 2015, https://perma.cc/RF6C-9NQT.

[58] *See* Eduard Kovacs, *Hacking Back: Industry Reactions to Offensive Security Research*, SECURITY WEEK, Nov. 13, 2015, https://perma.cc/28RR-BU37 (quoting reactions of Kaspersky Lab, Raytheon, RSA, etc.).

III. A BRIEF NOTE ON INTERNATIONAL LAW

No formal source of international law directly bars private sector actors, acting on their own, from using the active defense measures described above.[59] The first international treaty addressing crimes committed on the Internet, the Budapest Convention on Cybercrime,[60] calls on its signatories to criminalize a number of actions dealing with access to computer systems or interception of non-public computer data.[61] But the Budapest Convention is not self-executing, has been ratified by only sixty-two mostly-European states parties (many of whom ratified with reservations), and only hints at an emerging set of norms.[62]

[59] *See, e.g.*, Paul Rosenzweig, *supra* note 13. Rosenzweig generally concludes that "(1) To the extent any customary international law exists, it is likely to discourage private sector self-help outside the framework of state-sponsored action; and (2) almost certainly, hack back by a U.S. private sector actor will violate the domestic law of the country where a non-U.S. computer or server is located." *See also* CCHS report, *supra* note 14. *See also* Gary Brown and Keira Poellet, *The Customary International Law of Cyberspace*, STRATEGIC STUD. QUARTERLY 126 (Fall 2012), https://perma.cc/765N-CGY3, (quoting Anthea Roberts, "In situations not addressed by established consensus on what constitutes lawful behavior, nations may take actions they deem appropriate." They go on to note that customary international law in cyberspace is especially difficult to assess given the general "lack of protest from nations whose systems have been degraded in some way by obnoxious cyber activity" and liken most state cyber activity to espionage, which in peacetime is not a violation of international law and is not considered to violate sovereignty (although it may violate domestic law)).

[60] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185 (entered into force Jul. 1, 2004), https://perma.cc/GDU2-QX6L [hereinafter "Budapest Convention"].

[61] States parties are called to criminalize, inter alia, access without right to a computer system; intentional interception without right of non-public transmissions of computer data; intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right; intentional hindrance without right of the functioning of a computer system by the misuse of computer data; and the production, sale, procurement, import, or distribution or any device, program, or data such as a password or access code designed or adapted primarily for the purpose of committing the previous offenses. *Id*. arts. 2–6. The Budapest Convention's other provisions are generally outside the scope of this essay.

[62] U.S. ratification prompted criticism from all sides, but now those concerns seem to have been overblown. For a contemporaneous news article, *see, e.g.*, Nate Anderson, *"World's Worst Internet Law" Ratified by Senate*, ARS TECHNICA, Aug. 4, 2006, https://perma.cc/XTP6-GJWX. For a more recent article questioning the long-term efficacy of the Budapest Convention, *see* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER, https://perma.cc/S4NW-NU9H (telling a cautionary tale about what the Budapest Cybercrime Convention suggests for future cyber-treaties).

Paul Rosenzweig has argued[63] that the Budapest Convention's repeated use of the term "without right"[64] seems to contemplate the idea that states parties could reasonably permit otherwise unlawful cyber activity in their domestic laws if done pursuant to established legal defenses, excuses, or justification. This widely cited argument, however convincing from an American legal point of view, is so far merely academic; it has not yet and may never be raised before any formal body. And self-defense is itself an idea that is interpreted differently in different places, dependent as it is on malleable and culturally specific concepts like reasonableness and proportionate response (as is also true for other forms of legal defenses, excuses, and justifications).

The most widely cited of the "soft law" projects, the Tallinn 2.0 International Group of Experts, considered a hypothetical "case in which a corporation is the target of a malicious cyber operation by a State." The Group concluded that, as a matter of current international law, the "corporation does not violate the sovereignty of that State if it hacks back," reasoning that as a matter of international law only States bear the obligation to respect the sovereignty of other States, unless the non-State actor's actions are attributable to a State.[65] Attribution, of course, is difficult in cyberspace.[66]

[63] *See* Rosenzweig, *supra* note 13; *see also* Paul Rosenzweig, Steven Bucci, & David Inserra, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, HERITAGE BACKGROUNDER, May 5, 2017, http://report.heritage.org/bg3188. *See also* Sharon Cardash & Taylor Brooks, *Mounting an Active Defense Against Cyber Threats*, INTERNATIONAL PEACE INSTITUTE GLOBAL OBSERVATORY, Nov. 10, 2016, https://perma.cc/2ZR7-JV7V (two persons who worked on the CCHS Task Force, adopting Rosenzweig's argument).

[64] *See* Council of Europe, *Explanatory Report to the Convention on Cybercrime*, Nov. 23, 2001, https://perma.cc/FPF4-YVEE.

[65] TALLINN 2.0, *supra* note 6, Rule 4; *c.f.* Rules 15 and 17.

[66] The traditional citation for this point is a New Yorker cartoon of a dog sitting at a computer, telling another dog that "On the Internet, nobody knows you're a dog." That cartoon even has its own Wikipedia article, https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog. But as attributional analysis gets better, the cartoon is starting to show its age. Consider, for example, Google's or Check Point's analyses in Part II.b.(4), *supra*, or any of the various indictments by the U.S. DoJ of Chinese, Russian, Iranian, or North Korean hackers (or, for that matter, any indictments by those governments of U.S. personnel).

Outside the Budapest treaty framework and the unofficial Tallinn attempts at codifying the law as it is believed to exist today, several other international "soft law" projects have made headlines but have yet to see tangible results. The 2016–2017 United Nations Group of Governmental Experts, convened to consider applicable norms, failed to come to consensus.[67] Three other prominent examples have yet to move the needle in any meaningful way: Microsoft's call for a Digital Geneva Convention, which calls states to pledge not to attack private corporations;[68] the related Cybersecurity Tech Accord, signed by thirty-four companies, which promises not to help governments launch cyberattacks against innocent citizens and enterprises;[69] and the Paris Call for Trust and Security in Cyberspace, which among other things calls for "steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors."[70]

Analyses of international law in cyberspace have considered analogies to piracy, letters of marque, and private security, but all remain, for now, scholarly or think-tank projects.[71] States have yet to adopt these theories. For now, it seems the final word is

[67] *See, e.g.*, Adam Segal, *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?"*, COUNCIL ON FOREIGN RELATIONS BLOG, Jun. 29, 2017, https://perma.cc/T8JQ-WTW4; *see also* Arun Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE, Jul. 4, 2017, https://perma.cc/2WB6-JBDS.

[68] *See* Brad Smith, *The need for a Digital Geneva Convention*, MICROSOFT BLOG, Feb. 14, 2017, https://perma.cc/3M5H-4MPK.

[69] *See* Brad Smith, *34 companies stand up for cybersecurity with a tech accord*, MICROSOFT BLOG, Apr. 17, 2018, https://perma.cc/XC27-6ET2.

[70] Paris Call of 12 November 2018 for Trust and Security in Cyberspace, https://perma.cc/2Z5Q-9GE4. The 370 signatories include all 28 members of the European Union and 27 of the 29 NATO members. Paris Call signatories from the private sector include Microsoft, Google, Facebook, Intel, Citigroup, and Visa, among others.

[71] *See, e.g.*, Rosenzweig, *supra* note 13. *See also* Wyatt Hoffman & Ariel Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, CARNEGIE ENDOWMENT FOR INT'L PEACE, Jun. 14, 2017, https://perma.cc/X2DZ-YATV. Rosenzweig and others have also considered whether useful international norms may be gleaned from the ICTY's broad reading of the Rome Statute in *Kordic* and *Cerkez* (arguing that self-defense of property may be a rule of customary international law) or from historical analogies to the laws of piracy and letters of marque. Although these analogies come up often, no international norm has yet formed. And even if it should, Rosenzweig points out that historical practice

still that "until international agreements alter the law, or the International Court of Justice rules on such issues, many of the novel legal questions that cyber attacks pose will be answered by creative, if contrived, adaptation of historic doctrines."[72]

With international law functionally silent, we turn to domestic laws.

IV. A SURVEY OF DOMESTIC LAWS

a. Which countries should we look at?

As mentioned in Part I.c., one claim sometimes made in the conversation on active defense measures is that companies that operate in more permissive legal jurisdictions are driving this activity.[73] But which of these unnamed jurisdictions, exactly, are "permissive" and how might we identify them? Without doing a comprehensive global study covering over 196 jurisdictions (not counting sub-federal jurisdictions like the individual United States), how might we begin a reasonably expansive survey?

To create a manageable yet diverse list of countries whose laws might be worth exploring, I merged a number of rankings of states that lead across a broad set of cybersecurity measures,[74] states that are the home jurisdictions for the world's largest companies,[75] states that are the home jurisdictions for the world's cybersecurity

would not necessary empower private sector actors, but would subject them to additional state oversight, consistent with modern concepts of state responsibility. For more along this latter cautionary line of thinking, *see* Eichensher, *infra* note 189.

[72] Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attack*, 6 HARV. NAT'L SEC. J. 474, 511 (2015).

[73] *See* Hoffman, *supra* note 17.

[74] *See* International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017*, https://perma.cc/JH62-DPAR. *C.f.*, Bhaskar Chakravorti, Ajay Bhalla, & Ravi Shankar Chaturvedi, *60 Countries' Digital Competitiveness, Indexed*, HARV. BUS. REV., Jul. 12, 2017, https://perma.cc/CA66-5B4M.

[75] *See* PricewaterhouseCoopers (PWC), *Global Top 100 Companies* (2018), https://perma.cc/X8BK-BPZS.

companies,[76] states that are commonly said to be the world's most powerful state cyber powers,[77] and states that comprise the world's most powerful military powers generally.[78]

Twenty states appear repeatedly on those lists. I survey here this limited group: Australia, Canada, China, Estonia, France, Germany, Iran, Israel, Japan, the Netherlands, Oman, Russia, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan,[79] the U.K., and the U.S.[80] While understanding that any selection inevitably leaves out important players, within this diverse group of twenty we find large and small states, U.S. allies and non-allies, various forms of democracies and non-democracies, civil and common-law jurisdictions, twelve states party to the Budapest Convention and eight non-parties.

b. What questions should we ask?

As we saw in Part II, the U.S. conversation about the legality of active defense measures has generally centered around the constraints imposed by the Computer Fraud and Abuse Act (CFAA), which prohibits unauthorized accessing, changing, or deleting data in another's computer and transmitting code to another's computer;[81] the Wiretap Act, which prohibits intercepting communications without a court order (or equivalent

[76] *See* Cybersecurity Ventures, *Cybersecurity 500* (2018), https://perma.cc/33QQ-SRVJ?type=image (the methodology on which Cybersecurity Ventures made their selection of the "top 500" is publicly available here: https://perma.cc/KM86-XFFG).
[77] *See, e.g.*, Shannon Vavra, *The World's Top Cyber Powers*, AXIOS, Aug. 13, 2017, https://perma.cc/7SVG-NAGA (identifying China, Iran, Israel, North Korea, Russia, the U.S., and the U.K.).
[78] *See* Global Firepower, *2019 Military Strength Ranking*, https://perma.cc/8CLY-ENUZ.
[79] I take no position one way or another on the legal status of Taiwan other than acknowledging that it has a set of laws relevant here and is the home jurisdiction for some of the world's largest companies and vibrant cybersecurity companies. In this essay, any reference to Taiwan as a state should be read as referring to this footnote.
[80] No methodology is unassailable, but this merger of both subjective and objective rankings includes both the "big" cyber power states and diverse "others." If I were to expand the list based on the same criteria that created this list of twenty, the next five would be Egypt, Malaysia, Mauritius, Ireland, and Brazil.
[81] 18 U.S.C. § 1030 *et seq.*, penalizing anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any [Internet-connected computer]…[or] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes [any impairment to the integrity or availability of data, a program, a system, or information] without authorization, to [any Internet-connected computer]."

defined by law);[82] and the prohibition on "pen register" and "trap and trace" (PRTT) devices—devices or programs that collect, respectively, outgoing and incoming metadata.[83]

Our first question, then, is a basic one: which other states, if any, *have* parallel laws that might similarly restrict private sector activity? Although the question seems obvious, few in the U.S. ask it and fewer still go on to find and read the text of those laws.

Because most other states codify their law differently than in the U.S., I've organized those laws in Table 1, below, using a relevant framework from the Budapest Convention:[84]

(1) access without right to a computer system [which presumably constrains the use of beacons and certain traceback analysis methods];

(2) damaging, deletion, deterioration, alteration, or suppression of computer data without right [generally not implicated by mainstream active defense measures *except to the extent that* (A) careless or incompetent private sector actors employing active defense measures may cause damage recklessly or negligently and (B) beacons that execute code on another's computer are "altering data" in the course of executing the program];

[82] 18 U.S.C. § 2510 *et seq*.

[83] 18 U.S.C. § 3121.

[84] The Budapest Convention also calls on states parties to criminalize computer-related offenses such as forgery or fraud, content-related crimes (e.g., child pornography), and offenses related to intellectual property rights. Some of those offenses may constrain other active defense measures not addressed here. For example, intelligence gathering on certain portions of the dark web may involve investigators' viewing or trading in illicit material to gain trust or access to certain sites. This is understandably fraught in most jurisdictions. To limit this essay's (already broad) scope, here I address only the "offenses against the confidentiality, integrity and availability of computer data and systems" in Chapter II, Title 1 of the Convention. *See supra* note 60.

(3) interception without right of non-public transmissions of computer data [which presumably constrains the use of some sinkholes and honeypots]; and

(4) hindrance without right of the functioning of a computer system by the misuse of computer data [generally not implicated by active defense measures *except to the extent that* (A) careless or incompetent private sector actors contemplating active defense measures may cause damage recklessly or negligently and (B) beacons that execute code on another's computer are "altering data" in the course of executing the program].

In addition, most countries criminalize (5): the production, sale, procurement, import, or distribution or any device, program, or data such as a password or access code designed or adapted primarily for the purpose of committing the previous offenses. These last types of provisions have implications for public-private information sharing and security testing, so I've included them here as a relevant part of the map.

c. What do states formally and clearly prohibit?

Table 1 simply lays out which states have laws governing these five types of activity. Three administrative notes:

(1) In the Appendix to this essay I provide Bluebook citations with permalinks to the most recent English text or translation publicly available in 2019. Some translations are "official," some "unofficial"; in all cases, none have legal force in the respective jurisdiction.

(2) Because I have listed full citations elsewhere, I have generally not cluttered tables with footnotes in each cell of each table.

(3) In the body of this essay and in tables, I typically list states alphabetically by their common names. Their formal names are in the Appendix.

Table 1: Do states have laws formally and clearly prohibiting cyber activity?

State	**Does the domestic law prohibit, without right or authorization, a private sector actor doing the following on another's computer? *In all cases, yes.***				**Any prohibition on trade in programs that enable these offenses? *For the most part, yes.***	**Any laws that would explicitly permit or except active defense measures from the laws in the prior columns? *Only a handful.***
	Accessing data	**Changing or deleting data**	**Intercepting communications or metadata**	**Interference with normal computer functions**		
Australia	Criminal Code §§ 477.1 & 478.1	Criminal Code §§ 477.1 & 478.1	Telecommunications Act §§ 7 & 105	Criminal Code §§ 477.1 & 477.2	Criminal Code § 478.4	Telecommunications Act § 7 permits ISPs to trace any person suspected of computer crimes
Canada	Criminal Code § 342.1	Criminal Code § 430	Criminal Code § 342.1 & § 184	Criminal Code § 430	Criminal Code § 342.1 & 342.2	Criminal Code § 184(2)(e) permits ISPs to take reasonable protective measures
China	Criminal Law Art. 285	Criminal Law Arts. 285 & 286	Criminal Law Arts. 283, 285, & 286	Criminal Law Art. 286	Criminal Law Arts. 283, 285, & 286	
Estonia	Penal Code § 217	Penal Code § 206	Penal Code § 156	Penal Code § 207	Penal Code § 216[1]	Cybersecurity Act reserves active defense to the state
France	Penal Code Arts. 323-1 & 323-2	Penal Code Art. 323-3	Penal Code Art. 226-15; Code of Crim. Proc. Art. 706-102	Penal Code Art. 323-2	Penal Code Art. 323-3-1	*See Part IV.j. infra*
Germany	Criminal Code § 202a	Criminal Code § 303a	Criminal Code § 202b	Criminal Code § 303b	Criminal Code § 202c	
Iran	Criminal Code Art. 726 [1]	Criminal Code Arts. 731 [6] & 733 [8]	Criminal Code Art. 727 [2]	Criminal Code Arts. 734 [9] & 735 [10]	Criminal Code Art. 750 [25]	
Israel	Computers Law § 4	Computers Law § 2	Wiretap (Secret Monitoring) Law § 2	Computers Law §§ 2 & 3	Computers Law § 6	*Contemplated. See Part IV.d.(3) infra.*

State	**Does the domestic law prohibit, without right or authorization, a private sector actor doing the following on another's computer? *<u>In all cases, yes.</u>***				**Any prohibition on trade in programs that enable these offenses? *<u>For the most part, yes.</u>***	**Any laws that would explicitly permit or except active defense measures from the laws in the prior columns? *<u>Only a handful.</u>***
	Accessing data	**Changing or deleting data**	**Intercepting communications or metadata**	**Interference with normal computer functions**		
Japan	Unauthorized Computer Access Law [UCAL][85] Art. 3	Penal Code Arts 168-2, 234-2, & 259; UCAL Art. 3	Telecommunications Business Act Art. 4	Penal Code Arts. 168-2 & 234-2	Penal Code Arts. 168-2 & 168-3; [86] *See also Japan's reservations to the Budapest Convention*[87]	
Netherlands	Criminal Code Art. 138ab	Criminal Code Arts. 350a & 350b	Criminal Code Arts. 138c & 139d	Criminal Code Art. 138b	Criminal Code Art. 139d	Computer Crime Act III reserves active defense to the state
Oman	Cyber Crime Law Art. 3	Cyber Crime Law Arts. 3 & 9	Cyber Crime Law Art. 8	Cyber Crime Law Arts. 9 & 10	Cyber Crime Law Art. 11	
Russia	Criminal Code Arts. 159.6 & 272	Criminal Code Arts. 159.6 & 272	Criminal Code Arts. 138 & 274	Criminal Code Arts. 159.6 & 272	Criminal Code Art. 138.1 & 273	
Singapore	Computer Misuse Act § 3	Computer Misuse Act § 5	Computer Misuse Act § 6	Computer Misuse Act § 7	Computer Misuse Act § 8B	

[85] A common abbreviation. The full name is the "Act on Prohibition of Unauthorized Computer Access."

[86] Articles 168-2 and 168-3 were added to the Penal Code by Amendment June 24, 2011 Extraordinary Law No. 74 [Amendment of a law to amend a part of the Penal Code, etc. to cope with the advancement of information processing, etc.]. Both are still valid law, but erroneously are not incorporated into the Japanese Law Translation site that the rest of the Japanese laws here are drawn from. Harvard Law Library reported this error to the Japanese Ministry of Justice in April 2019. Any translation of those articles used herein comes from the EHS Law Bulletin Series II (PA 37) 2011.

[87] Japan reserved the right not to apply Article 6, paragraph 1, except for: (a) the offences set forth in Article 168-2 or Article 168-3 [*see id*] of the Penal Code; and (b) the offences set forth in Article 4, 5, and 6 of the UCAL.

State	**Does the domestic law prohibit, without right or authorization, a private sector actor doing the following on another's computer?** ***In all cases, yes.***				**Any prohibition on trade in programs that enable these offenses?** ***For the most part, yes.***	**Any laws that would explicitly permit or except active defense measures from the laws in the prior columns?** ***Only a handful.***
	Accessing data	**Changing or deleting data**	**Intercepting communications or metadata**	**Interference with normal computer functions**		
South Korea	Network Act[88] Art. 48(1) ; Infrastructure Protection Act[89] Art. 12	Network Act Art. 48(2); Infrastructure Protection Act Art. 12	Network Act Art. 49	Network Act Art. 48(3); Infrastructure Protection Act Art. 12	Network Act Art. 48(2)	Article 48-2 contemplates state supervision of ISP private sector “countermeasures”
Spain	Penal Code Arts. 197 & 197 bis	Penal Code Art. 197 & 264	Penal Code Arts. 197 & 197 bis	Penal Code Art. 264 bis	Penal Code Arts. 197 ter, 248, and 264 ter	
Sweden	Penal Code 4:9c	Penal Code 4:9c	Penal Code 4:8	Penal Code 4:9c	Mere trade not prohibited, unless done in preparation for data breach	
Switzerland	Criminal Code Art. 143	Criminal Code Art. 144bis	Criminal Code Art. 143	Criminal Code Art. 144bis	Criminal Code Art. 143bis & 144bis	
Taiwan	Criminal Code Art. 358	Criminal Code Art. 359	Communication Security & Surveillance Act Art. 24	Criminal Code Art. 360	Criminal Code Art. 362	Communication Security & Surveillance Act reserves active defense to the state
U.K.	Computer Misuse Act § 1	Computer Misuse Act § 3	Investigatory Powers Act § 3	Computer Misuse Act § 3	Computer Misuse Act § 3A	Investigatory Powers Act reserves active defense to the state
U.S.	18 U.S.C. § 1030(a)(2)(C)	18 U.S.C. § 1030(a)(5)(A)	18 U.S.C. § 2511; 18 U.S.C. § 3212	18 U.S.C. § 1030(a)(5)	18 U.S.C. § 1029	*Contemplated. See Part IV.d.(3) infra.*

[88] The full name is the “Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.”

[89] The full name is the “Act on the Protection of Information and Communications Infrastructure.”

d. Preliminary comments from Table 1.

Before going into more detail, I want to pause for four very basic points regarding organization, coverage, active-defense specific laws, and extraterritorial jurisdiction.

(1) Organizational diversity

There is no "model cyber code." The laws surveyed here rarely mirror each other in word choice or in organization. Most states cover cyber issues comprehensively in their criminal code, while others have a standalone computer code (i.e., Iran, Israel,[90] Japan, Oman, Singapore, and the U.K.). Several place the general prohibition on intercepting communications in transit in their respective government surveillance codes (i.e., Israel, Taiwan, the U.K., and the U.S.) or in their telecommunications code (i.e., Australia and Japan). Sweden uses thirteen lines of text to cover the same substantive crimes as Australia covers in eight pages. Singapore explicitly copied portions of its law from other countries, but then went on to add its own unique innovations.

At an organizational level, one point is particularly striking: whether a state is party to the Budapest Convention has little discernable relationship with the way that state chooses to codify, phrase, and organize its cyber laws. In their domestic laws the Budapest states parties rarely mirror the phrasing of the Budapest Convention's substantive Articles 2 through 6.[91] And many of the Budapest states parties surveyed here issued reservations on substantive or jurisdictional points (or both).

[90] For one account of how and why Israel chose to draft a comprehensive Computers Law, *see* Miguel Deutch, *Computer Legislation: Israel's New Codified Approach*, 14 J. MARSHALL J. COMPUTER & INFO. L. 461 (1996), https://perma.cc/5HQD-MS92. That article also includes some interesting comments on the U.K.'s Computer Misuse Act.
[91] Budapest Convention, *supra* note 60.

For reference,[92] China, Iran, Oman, Russia, Singapore, South Korea, Sweden, and Taiwan are not party to the Budapest Convention. Australia, Canada, Estonia, France, Germany, Israel, Japan, the Netherlands, Spain, Switzerland, the U.K., and the U.S. are. Yet non-party Singapore's laws, for example, have far more in common with Canada's laws than Canada's laws have with, say, the German or Japanese laws. By the same token, the German and Chinese laws have more in common, in both coverage and structure, than either has with the U.S. law.

(2) Broadly similar coverage

In Parts IV.e. through IV.j., *infra*, I go into further detail about where the laws are more subtly distinct. Yet before discussing differences, it's important to note that there are no obvious gaps, empty boxes, or obviously "permissive" jurisdictions in this initial survey. What are we to make of this? One response might be that even though formal international law has so far failed to harmonize laws globally, the realities of cyberspace have imposed their own logic in domestic law.[93] Because there are only so many things one can do in cyberspace, any state that wants to respond to the real world effects of cyber incidents comes inevitably to prohibit the same sorts of things. If there are indeed more "permissive" states, it either is a matter of degree rather than a binary "permissive" versus "strict" distinction—or a matter of a state choosing to be informally permissive by exercising prosecutorial discretion.

[92] The list of signatories can be found here: https://perma.cc/4F6U-QZCX. Interestingly, Sweden signed but did not ratify the Convention.

[93] Another facet of the now-foundational insight that "Code is law." LAWRENCE LESSIG, CODE 2.0 (2006), http://www.codev2.cc/.

(3) No explicit "active defense" laws

No country surveyed has any formal law providing an explicit legal defense for private sector actors contemplating active defense measures, such as the U.S. Congress is now contemplating.[94] If the U.S. were to pass something like H.R. 4036, it would be an immediate outlier.[95] Like the U.S., Israel has draft active defense language in a bill under consideration[96] but, as in the U.S., nothing is yet law. I could not find any country other than the U.S. and Israel where such proposed legislation is under consideration.[97]

By contrast, some states have structures and procedures for government oversight of Internet Service Providers (ISPs) monitoring Internet communications and even taking "intrusion countermeasures." Some permit their ISPs to act under various degrees of state oversight (e.g., Australia, Canada, and South Korea) while others (e.g., Estonia, the Netherlands) explicitly reserve the right to employ active defense measures to the state. A number of states have guidelines for imposing criminal liability rules on corporations or groups. I discuss these further in Part. IV.j., *infra*.

[94] The Craig, Shackelford, and Hiller study, *supra* note 19, focused on only one type of law (unauthorized access) in eight countries (the G8), but came to a similar conclusion.

[95] *See supra* note 16.

[96] "Section 64 of the proposed Cyber Defense and National Cyber Directorate Bill proposes an exemption from liability for unlawful wiretapping, invasion of privacy, or intrusion into computers, if an organization takes steps in furtherance of cybersecurity, maintains a cybersecurity policy and is transparent to affected individuals about its use of cybersecurity measures." Haim Ravia and Dotan Hammer, *Israel: Cybersecurity 2019*, INTERNATIONAL COMPARATIVE LAW GUIDE, Oct. 16, 2018, https://perma.cc/HQ6X-NW72. For more on the proposed bill (which in greater part addresses state powers), *see* Haim Ravia, *Memorandum of Israeli Cyber Law Published Today, with Far-Reaching Powers*, LAW.CO.IL BLOG, Jun 20, 2018, https://perma.cc/N3YU-TYZF.

[97] Craig, Shackleford, & Hiller, *supra* note 19, examined an example from Singapore of a quasi-private sector active defense law—one that then permitted the state to authorize or direct specified private persons to take any measure that the state could take to protect a computer or a network. Note that the law they identified in 2015 was moved in 2018 as a major cybersecurity law recodification. For the 2013–2018 law, *see* Computer Misuse and Cybersecurity Act 1993, c. 50A § 15A, https://perma.cc/RBR6-WMY2. For current law, refer to Computer Misuse Act 1993, c. 50A § 1–9, https://perma.cc/4WGF-9Y58 and Cybersecurity Act 2018, § 23, https://perma.cc/XKC6-3US9.

(4) Extraterritorial jurisdiction

Comparative jurisdiction deserves its own intense study.[98] The relevant U.S. laws were made explicitly extraterritorial in 2001.[99] For purposes of this essay, I just note that most of the states surveyed assert extraterritorial jurisdiction, in some form or another, over computer crimes. This is most commonly done with "territorial effects" language such as "A crime is deemed to have been committed where the criminal act was perpetrated and also where the crime was completed or, in the case of an attempt, where the intended crime would have been completed."[100]

A few countries have slightly more nuanced rules or phrasings. Iran provides jurisdiction over any crimes where the data involved was in any way stored in or carried through Iranian telecommunications systems.[101] Japan, interestingly, asserts jurisdiction by reference to the Budapest Convention.[102] Singapore's extraterritorial jurisdiction language encompasses not only cases where the "computer, program or data was in

[98] For theories of how extraterritorial jurisdiction may be justified, *see generally Research in International Law, Draft Convention on Jurisdiction with Respect to Crime*, 29 AM. J. INT'L L. 437 (Supp. 1935).

[99] *See* DoJ Manual *supra* note 38 at 115–116.

[100] BROTTSBALKEN [BrB] [PENAL CODE] 2:4 (Swed.). For states with similar language, *see also* Zhonghua Renmin Gongheguo Xingfa (中华人民共和国刑法) [Criminal Law of the People's Republic of China] art. 6 (China); KARISTUSSEADUSTIK (Penal Code), c. 1 § 11 (Est.); CODE PÉNAL [C. PÉN.] [Penal Code] art. 113-2 (Fr.); STRAFGESETZBUCH [STGB] [Penal Code] § 9 (Ger.); Royal Decree No. 12, Feb. 6, 2011, Issuing the Cyber Crime Law, art. 2 (Oman); UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] arts. 11 & 12(3) (Russ.); SCHWEIZERISCHES STRAFGESETZBUCH [STGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757, art. 8.3 (Switz.); Zhōnghuá mínguó xíngfǎ (中華民國刑法) [Criminal Code of the Republic of China] 1935, art. 4 (Taiwan); Computer Misuse Act 1990, c. 18, § 4 (UK).

[101] MAJMUAHI QAVAINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1381 [2002], art. 753 [corresponding to Computer Crime Act 1388 [2009] art. 28] (Iran).

[102] The relevant Japanese law generally does not embrace extraterritorial jurisdiction, except where the UCAL refers to Penal Code Art. 4-2, which in turn establishes that the Code will apply to crimes committed "governed by a treaty even if committed outside the territory of Japan." KEIHŌ (PEN. C.) 1907, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan). Because Japan is a Budapest Convention party, these nested provisions apparently provide the requisite "hook." *See also* Hiromi Hayashi (of Mori Hamada & Matsumoto, one of the "Big Four" law firms in Japan), *Japan: Cybersecurity 2019*, INTERNATIONAL COMPARATIVE LAW GUIDE, Oct. 16, 2018, (indicating that this is indeed how Japanese law asserts extraterritorial jurisdiction) https://perma.cc/EN77-9RGR.

Singapore at the material time" but also cases where "the offence causes, or creates a significant risk of, serious harm in Singapore."[103] By contrast, Canada, the Netherlands, and South Korea don't precisely define what it means to commit a crime "in" their territory (i.e., they lack statutory language stating that a crime is committed where its effects are felt), but may be read broadly to accomplish the same effect.

e. Nuances in unauthorized access laws

Broadly speaking, laws that prohibit access without right to a computer system presumably constrain the use of beacons and certain traceback analysis methods. Every state surveyed prohibits unauthorized access to data at rest on another's computer. The key substantive difference is whether the prohibition on unauthorized access applies to all computer data, or only to that data protected by security measures (e.g., by a password).

This distinction seems outdated—who in 2019 could forget to secure their data with the most basic of security measures? But it turns out that the Internet is littered with unprotected data and servers. One recent headline demonstrates the point: on April 3, 2019, security firm UpGuard announced that records of over 540 million Facebook users (in two different datasets) had been left exposed on public servers hosted by Amazon.[104] UpGuard notified the owner of the larger dataset (with over 500 million records) on January 10, 2019 and, hearing no response, notified Amazon Web Services on January 28. The larger dataset was not secured until Bloomberg contacted Facebook for comment on April 3.[105]

[103] Computer Misuse Act 1993, c. 50A § 11(3) (Sing.) (where serious harm is defined with a number of examples—a unique facet of Singaporean law, akin to how some U.S. federal agencies publish examples in the Federal Register of how they interpret their own regulations). Singapore expanded its jurisdictional language in 2018. *See supra* note 97.

[104] *Losing Face: Two More Cases of Third-Party Facebook App Data Exposure*, UPGUARD, Apr. 3, 2019, https://perma.cc/K6SE-PLPG.

[105] *Id.*

The U.S. CFAA bans unauthorized access to *all* computer data.[106] Of the states surveyed here, that ban puts the U.S. in a group with Canada,[107] China,[108] France,[109] Israel,[110] Oman,[111] Russia,[112] Singapore,[113] South Korea,[114] Sweden,[115] and the U.K.[116] By contrast, eight states criminalize access to data only if it is protected by a security

[106] 18 U.S.C. § 1030(a)(2). *See also* DoJ Manual, *supra* note 38 at 5–12 & 16–22 (explaining the contours of how "unauthorized" and "access" have been interpreted in various jurisdictions and under various policy rationales, but drawing no bright-line distinction between access to secured versus unsecured data).

[107] "Everyone is guilty of an indictable offence…who, fraudulently and without colour of right, …obtains, directly or indirectly, any computer service…" where "computer service includes data processing and the storage or retrieval of computer data…" Canada Criminal Code, R.S.C. 1985, c C-46 § 342.1.

[108] "Whoever…intrudes into a computer information system other than [state affairs, national defense, or science and technology] or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system…shall, if the circumstances are serious, be sentenced…" Zhonghua Renmin Gongheguo Xingfa (中华人民共和国刑法) [Criminal Law of the People's Republic of China], art. 285 (China).

[109] "Fraudulently accessing or remaining within all or part of an automated data processing system is punished by…" Code Pénal [C. pén.] [Penal Code] art. 323-1 (Fr.).

[110] "Whoever unlawfully penetrates computer material that is in a computer shall be liable…" Computers Law 5755-1995, § 4, A.G. Pub., 2015 (Isr.). The Israeli Supreme Court has read this section in the broadest possible sense, covering any access without clear permission or other legal authority. *See* Leave for Criminal Appeal 8464/14 *The State of Israel v. Ezra* (*matter of Nir Ezra*). For commentary and summary in English *see* Dotan Hammer, *Israeli Supreme Court Determines What Is Considered Unlawful Intrusion to Computers*, Law.Co.Il Blog, Dec. 18, 2015, https://perma.cc/8BS5-VFHP.

[111] "Everyone who intentionally and illegally access an electronic site or informational system or information technology tools or part of it or exceeded his authorized access to it or continued his existence therein after being aware of his access, shall be punished." Royal Decree No. 12, Feb. 6, 2011, Issuing the Cyber Crime Law, art. 3 (Oman) [sic].

[112] "Illegal access to legally-protected computer information, if this deed has involved the…copying of computer information, - is punishable…" Ugolovnyi Kodeks Rossiiskoi Federatsii [UK RF] [Criminal Code] art. 272 (Russ.). *See generally* Vasily Torkanovskiy, *Russia*: *Business Crime 2019*, International Comparative Law Guide to Business Crime Laws and Regulations, Dec. 9, 2018, https://perma.cc/2MAP-ZMNK ("Article 272 prohibits unauthorized access to digital information (in the broadest sense) protected by law where such interference leads to destruction, blocking, alteration or copying of the information").

[113] "…any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence…" Computer Misuse Act 1993, c. 50A § 3 (Sing.).

[114] "No one shall intrude on an information and communications network without a rightful authority for access or beyond a permitted authority for access." Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. [commonly known as the Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, art. 48(1), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.).

[115] "A person who…unlawfully obtains access to a recording for automatic data processing…shall be sentenced for breach of data secrecy…" Brottsbalken [BrB] [Penal Code] 4:9c (Swed.).

[116] "A person is guilty of an offence if—(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; [and he knows that] (b) the access he intends to secure, or to enable to be secured, is unauthorized…" Computer Misuse Act 1990, c. 18, § 1 (UK).

measure (Australia,[117] Estonia,[118] Germany,[119] Iran,[120] Japan,[121] Netherlands,[122] Switzerland,[123] and Taiwan[124]) or if unrestricted data is accessed predicate to another offense (Australia[125]).

Those groupings aren't inherently obvious—a theme echoed in the next several sections. The fault line does not fall along democratic / non-democratic or Western / non-Western lines (or any other obvious contrast). Of note, one longstanding argument in the U.S. legal academy is that the CFAA should be amended to "limit the scope of unauthorized access statutes to circumvention of code-based restrictions on computer

[117] "A person is guilty of an offence if: (a) the person [intentionally] causes any [knowingly] unauthorised access to…restricted data…" *Criminal Code Act 1995* (Cth) ch 10 pt 6 s 478.1 (Austl.). [Underscore here and in successive related footnotes added for emphasis.]
[118] "Illegal obtaining of access to computer systems by elimination or avoidance of means of protection is punishable…" KARISTUSSEADUSTIK (Penal Code), c. 13 § 217 (Est.).
[119] "Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable…" STRAFGESETZBUCH [STGB] [Penal Code] § 202a (Ger.).
[120] "Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished…" MAJMUAHI QAVAINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1381 [2002], art. 726 [Computer Crime Act art. 1] (Iran).
[121] "It is prohibited for any person to engage in an Act of Unauthorized Computer Access…" where a required element of unauthorized computer access is having an "access control feature." Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, art. 3, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan).
[122] "Unlawful entry shall be deemed to have been committed if access to the computerised device or system is gained: a. by breaching a security measure, b. by a technical intervention, c. by means of false signals or a false key, or d. by assuming a false identity." Art. 138ab SR (Neth).
[123] "Any person who … obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which…has been specially secured to prevent his access is liable…" SCHWEIZERISCHES STRAFGESETZBUCH [STGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757, art. 143 (Switz.).
[124] "A person who without reason by entering another's account code and password, breaking his computer protection, or taking advantage of the system loophole of such other accesses his computer or relating equipment shall be sentenced…" Zhōnghuá mínguó xíngfǎ (中華民國刑法) [Criminal Code of the Republic of China] 1935, art. 358, *translated in* Laws & Regulations Database of The Republic of China, https://law.moj.gov.tw/Eng/index.aspx (Taiwan).
[125] *See Criminal Code Act 1995* (Cth) ch 10 pt 6 s 477.1 (Austl.), which prohibits access to any computer data, without reference to whether it is secured or restricted, if "the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory…" where serious offense is defined as an offense "punishable by imprisonment for life or a period of 5 or more years." *See also* Tony Krone, *Hacking Offenses*, AUSTRALIAN INSTITUTE OF CRIMINOLOGY HIGH TECH CRIME BRIEF, 2005 (describing the history of Australia's decision to set a higher bar for criminalizing access), https://perma.cc/24XQ-GA5C.

privileges," as is done in the latter group of eight countries.[126] This survey would seem to indicate that it's an option to take seriously.

Within these broad categories there are finer distinctions. Spain is unusual in that it has fine-tuned rules for both specially protected data[127] and for any access to (unprotected but) private data generally.[128] Oman generally prohibits any unauthorized access but also goes on to provide separate aggravated penalties if the data accessed is "personal," medical, or banking-related.[129] Singapore and the U.K. make clear that it is "immaterial that the act in question is not directed at —(a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer."[130] Several states have thorough definitions for the key term "unauthorized"[131] while some, including the U.S., leave it undefined (which is either "plain understanding" or "vague" depending on one's point of view).

Table 2 further breaks down the offense of unauthorized access, showing how different states choose to penalize the crime based on certain discrete or aggravating factors. Comparing maximum penalties is a crude proxy for how seriously each state

[126] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003), https://perma.cc/R4C2-6MDQ. *See also* CCHS Report, *supra* note 14 at 39, Appendix I: Additional Views of Nuala O'Connor (arguing that the line between lawful active defense and unlawful "hacking back" should be the act of gaining unauthorized access, provided that a "circumvention of technical access control" element is added to the relevant part of the CFAA).

[127] CÓDIGO PENAL [C.P.] [Penal Code] art. 197 bis (Spain) ("Whoever by any means or procedure, violating the security measures established to prevent it, and without being duly authorized, accesses or facilitates another's access to the whole or a part of an information system or remains in it against the will of those who have the legitimate right to exclude them, will be punished…").

[128] CÓDIGO PENAL [C.P.] [Penal Code] art. 197 (Spain) (protecting data of a "personal or family nature" accessed "by any means").

[129] Royal Decree No. 12, Feb. 6, 2011, Issuing the Cyber Crime Law, art. 3–6 (Oman).

[130] Computer Misuse Act 1993, c. 50A, § 3 (Sing.) and Computer Misuse Act 1990, c. 18, § 1 (UK).

[131] *See, e.g.*, *Criminal Code Act 1995* (Cth) ch 10 pt 6 s 476 (Austl.); Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, art. 2, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan); Computer Misuse Act 1993, c. 50A, § 2(2)–(8) (Sing.)

views the offense, but in the absence of reliable data about actual prosecutions, is the best measure we have.

Note that in Table 2, "--" denotes only that the state does not have a specific provision addressing that type of unauthorized access, although broader laws may logically incorporate more specific ones. For example, Canada has the most straightforward of any state's penal provision: every type of unauthorized access is punishable by up to ten years in prison, whether the data accessed is unrestricted, restricted, or government or critical infrastructure data.

Table 2: Unauthorized access—maximum penalties[132]

State	Simple access	Access to restricted data	Access to government or critical infrastructure data
Australia	n/a	2 years	5 years [to life][133]
Canada	10 years	--	--
China	3 years	--	3 years
Estonia	n/a	3 years	5 years
France	2 years	--	5 years
Germany	n/a	3 years	--
Iran	n/a	91 days–1 year	--
Israel	3 years	--	--
Japan	n/a	3 years	--
Netherlands	n/a	1–4 years	--
Oman	1–6 months	--	1–3 years
Russia	2 years	--	2–5 years

[132] To avoid filling up the bottom of each page with endless citations (as in *supra* pages 32–33), here and in successive pages I generally only footnote particularly interesting points. Other citations can be traced by referring to Table 1 and the Appendix.

[133] The penalty only goes above five years if the access is done in pursuit of another serious offense, at which point the access crime takes on the penalty provisions of that serious offense (even if committing the serious offense is impossible).

Singapore	2 years	--	--
South Korea	5 years	--	10 years
Spain	1–4 years[134]	--	--
Sweden	2 years	--	--
Switzerland	n/a	5 years	--
Taiwan	n/a	3 years	4.5 years
U.K.	2 years	--	--
U.S.	5 years[135]	--	10 years

The most striking takeaway from this comparison is how low, from a U.S. perspective, the possible sentences are. The U.S. and Canadian laws fall at the high end of the spectrum, along with China, South Korea, and Switzerland. By contrast, every other state, whether democratic or autocratic, has penalties in the one- to three-year range.

f. Nuances in modifying data laws

Active defense measures as defined by the CCHS report and similar mainstream projects often explicitly exclude aggressive "hack-backs." However, laws that prohibit damaging, deletion, deterioration, alteration, or suppression of computer data without right are a necessary part of the discussion around active defense measures *to the extent that* (A) careless or incompetent private sector actors contemplating active defense measures may cause damage recklessly or negligently and (B) beacons that execute code on another's computer "alter data" in the course of doing so.

[134] *See supra* notes 127 & 128.

[135] The penal provisions of 18 U.S.C. § 1030(c) are the most complex of any of the states surveyed and cannot fit in a single spreadsheet cell. That subsection provides for sentences of up to twenty years depending on the information accessed, whether the offender had committed a prior offense, the effects of the offense, etc. "Simple" unauthorized access with any other factors is punishable by a single year in prison, whereas access to classified government data with aggravating factors is punishable by twenty years in prison (per count). Everything else falls somewhere in between. The DoJ Manual, *supra* note 38 at 3, provides a helpful chart to keep track of the various factors.

Unsurprisingly, all states surveyed prohibit changing, deleting, or inserting data, or executing code, on another's computer. Some states place their modifying data laws in a separate part of their respective codes from their computer access and interference sections. Based on the chapter headings, this approach suggests those states think about modifying data as akin to traditional mischief or fraud.[136]

The respective state codes incorporate a dizzying array of aggravating factors that affect what the appropriate punishment is for changing or deleting data. Almost every state has at least one sentencing category for "simple" unauthorized changing or deleting data and one category for more "serious" crimes; many have several layers of "seriousness."[137] Yet in relatively few cases are the degrees of seriousness defined with any precision. For example, the phrase "if the circumstances are serious" recurs 154 times in the P.R.C. Criminal Law (8th Amendment) to identify when higher penalty levels are triggered, but what makes those circumstances "serious" is not defined by law.[138] By contrast, Russia has one of the very few laws that defines "major damage" with a specific value: as exceeding one million rubles.[139]

The German law, to give another example, gives no firm criteria for distinguishing between the basic crime of deleting data, punishable by three years

[136] *See, e.g.*, Arts. 350a & 350b SR (Neth.) (where destruction or altering of computer data falls within the portion of the code that covers destruction of property generally, whereas other sections surveyed here fall in the trespass, eavesdropping, and privacy portions of the code); Canada Criminal Code, R.S.C. 1985, c. C-46 art. 430 (Can.) (where "mischief in relation to computer data" is a subparagraph within the basic crime of mischief or destruction of property); and KEIHŌ [PEN. C.] 1907, arts. 161-2, 234-2, 246-2, & 259 (Japan) (all of which in different ways frame the crime as one of harm to a business, property, right, or duty; in general, the Japanese law focuses on the harm that flows from access, rather than on the access itself).

[137] *But see* Canada Criminal Code, R.S.C. 1985, c C-46 arts. 342.1 & 450 (Can.) (making most computer crimes punishable by up to ten years in prison, without gradations).

[138] *See generally* Zhonghua Renmin Gongheguo Xingfa (中华人民共和国刑法) [Criminal Law of the People's Republic of China] (China).

[139] UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 272 note 2 (Russ.). For context, as of April 2019, one million rubles is between fifteen and sixteen thousand U.S. dollars.

imprisonment, and a similar act that harms an operation that is "of substantial importance for another's business, enterprise or a public authority," punishable by five years. But it does get (somewhat) more precise in setting forth examples of "especially serious cases," punishable by up to ten years:

> An especially serious case typically occurs if the offender
>
> 1. causes major financial loss,
> 2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
> 3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.[140]

Because the factors each country considers relevant vary so widely and the lines between each penalty level are so indistinct, a comparison of every factor in every state is impossible in limited space. But it is comparatively easy to contrast the way each state thinks about the low and high ends of the spectrum, by comparing the maximum penalties for a "simple" altering-data crime compared to the same crime with serious consequences or performed against critical infrastructure.

Table 3 demonstrates that with respect to the prohibition on altering data, the U.S. is again at the far right of the spectrum, along with Canada, China, South Korea, and the U.K.—but also that every country has a substantial jump in its maximum penalties when aggravating factors are present. Using maximum penalties as a crude proxy for seriousness, the reasonable conclusion is that all twenty states surveyed take modifying data similarly seriously, at least with regards to attacks on government or critical infrastructure.

[140] STRAFGESETZBUCH [STGB] [Penal Code] § 303b (Ger.). *Compare with* yet vaguer language in Sweden, "When assessing whether the crime is serious, it must be especially considered if the act has caused serious damage or affected a large number of data or otherwise been of a particularly dangerous nature." BROTTSBALKEN [BRB] [PENAL CODE] 4:9c (Swed.).

Table 3: Modifying data—maximum penalties

State	Unauthorized modification of data	Unauthorized modification of data with aggravating factors
Australia	2 years	10 years (or 5 years to life, if done with intent to commit a subsequent offense)
Canada	10 years	--
China	5 years	Minimum of 5 years
Estonia	3 years	5 years
France	3–5 years	5–10 years
Germany	2 years	3–10 years
Iran	6 months – 2 years	3–10 years
Israel	3 years	3–5 years
Japan	5 years	7–10 years
Netherlands	2 years	3–5 years
Oman	1–3 years	3–10 years
Russia	4 months (or 2 years labor)	4–7 years
Singapore	3 years	7–10 years
South Korea	7 years	10 years
Spain	6 months–3 years	2–5 years
Sweden	2 years	6 months minimum to 6 years maximum
Switzerland	3 years	1–5 years
Taiwan	5 years	7.5 years
U.K.	10 years	10 years to life
U.S.	10 years	5 years to life

g. Nuances in interception laws

Recall that, in the U.S. context, the use of certain active defense measures such as sinkholes or honeypots is generally thought to violate the Wiretap Act’s prohibition on intercepting (the substance of) private communications and the general prohibition on (the collection of metadata using) pen register and trap and trace devices. But here, too, the U.S. is by no means alone.

As Table 1 indicated, all states surveyed have a general prohibition against intercepting data in transit across the Internet and most place it in their criminal codes. Australia and Japan place the prohibition in their telecommunications codes, whereas France, Israel, the U.K., and the U.S. place the prohibition in their respective laws governing state wiretapping.[141] Canada, China, Singapore, South Korea, Switzerland, Taiwan, and the U.S. still sit at the high end of the spectrum (see Table 4).

Table 4: Intercepting data—maximum penalties

State	Penalty for intercepting data in transit
Australia	2 years
Canada	5–10 years
China	3–7 years
Estonia	Fine only
France	1 year
Germany	2 years
Iran	6 mo – 2 years
Israel	3 years
Japan	2 years
Netherlands	2 years
Oman	1 mo – 1 year
Russia	1– 2 years
Singapore	3–7 years
South Korea	5 years
Spain	3 mo – 2 years
Sweden	2 years
Switzerland	5 years
Taiwan	5 years
U.K.	2 years
U.S.	5 years

[141] For a chart listing states with lawful intercept capability laws, *see* Ian Brown, *Lawful Interception Capability Requirements*, SOC'Y FOR COMPUTERS & L., Aug. 13, 2013, https://perma.cc/2GEB-GE46. Strictly speaking, France's section is in its Penal Code, but is grouped in a completely different section as part of a constellation of laws around wiretapping.

Substantively, Switzerland is unique in that, unlike other states surveyed, it only prohibits intercepting data in transit that is "specially secured," just as it protects only specially secured data at rest from unlawful access.[142] France and Japan stand out in being the only countries surveyed that penalize intercepting data in transit less severely than accessing data at rest.[143]

Estonia is an interesting outlier because its Electronic Communications Act includes a whole chapter detailing how communications firms are required to secure their networks against third parties accessing data or metadata.[144] That Act specifically prohibits third persons from intercepting information by means of radio equipment.[145] But neither the Electronic Communications Act nor the Penal Code contain a similar explicit prohibition on intercepting telecommunications made over the Internet. The parallel provision we would expect to see in such an advanced Internet state is simply not in its obvious place.

[142] SCHWEIZERISCHES STRAFGESETZBUCH [STGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757, art. 143 (Switz.).

[143] In France, the maximum sentences are set at 1 year for intercepting data in transit versus 2–5 years for simple access to data at rest. *Compare* CODE PÉNAL [C. PÉN.] [Penal Code] art. 226-15 *with* art. 323. In Japan, the maximum sentences are set at 2 years for interception versus 3 years for accessing password-protected data at rest (as noted above, Japan does not penalize simple access to unprotected data). *Compare* Denki tsūshin jigyō-hō [Telecommunications Business Act] Act No. 86 of 1984, arts. 4 & 179, *with* Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, art. 3.

[144] ELEKTROONILISE SIDE SEADUS (Electronic Communications Act) 2005, c. 10 (Est.), https://perma.cc/C3P3-NQUL.

[145] *Id*., § 22 provides that "(1) It is prohibited to send, by means of radiocommunication, incorrect or misleading messages which may prejudice the safety of aircraft, ships or vehicles on land or of persons or the functioning of the activities of any rescue service agency. (2) It is prohibited for third persons to intercept information by means of radio equipment, except in the cases provided by law. (3) It is prohibited to process, and to use and disseminate, illegally intercepted information." Radio communication is defined as that "in which electromagnetic waves propagating in open space are used as the information carrier." *Id*., § 22(44).

Instead, Estonia has *constitutionalized* the right to confidential messages[146] and prosecutes such activity under the general "Violation of confidentiality of messages" provision of the Penal Code.[147] But counterintuitively, that provision warrants only an *unspecified fine* in most circumstances. Estonia's decision to be less specific in its penal prohibitions may reflect both a dedication to the free and open Internet model[148] and a preference for placing the cybersecurity liability burden squarely on telecommunications providers, while still complying with its constitutional treaty obligations.[149] Estonia regulates Internet content lightly, but telecommunications cybersecurity heavily.[150]

h. Nuances in computer interference laws

As with laws prohibiting modifying data, laws prohibiting computer interference are not definitionally relevant to active defense measures (as defined by the CCHS Report and similar mainstream projects). But they may still constrain the use of active defense measures *to the extent that* even technologically advanced actors must acknowledge that there is always a risk of error when using such measures.

[146] EESTI VABARIIGI PÕHISEADUS (Constitution of the Republic of Estonia) 1992, § 43. "Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means."

[147] "Violation of the confidentiality of a message communicated by a letter or other means of communication is punishable by a pecuniary punishment." KARISTUSSEADUSTIK (Penal Code), c. 13, § 156 (Est.). *See* Riigikohus [Supreme Court] Case #: 3-1-1-93-15 (Est.), https://perma.cc/HQM8-GKZF (stating that e-mails in transit are protected by § 43 of the Constitution and § 156 of the Penal Code) (in Estonian).

[148] *C.f.*, *Estonia Freedom on the Net Country Profile*, FREEDOM HOUSE, 2017, https://perma.cc/S37M-KKC5 (indicating that Estonia has one of the most lightly-regulated yet robust telecommunications industries in the world).

[149] The Estonian Constitution treats ratified treaties as valid law irrespective of whether they are transposed into its organic law. *See* EESTI VABARIIGI PÕHISEADUS (Constitution of the Republic of Estonia) 1992, §§ 3 & 123.

[150] Both the Electronic Communications Act, *supra* note 144, and the new Cybersecurity Act 2018 (KÜBERTURVALISUSE SEADUS, https://perma.cc/YY2H-UQ2A), provide for significant state oversight of Internet service providers' cybersecurity. For an overview of Estonian information technology laws, *see* Mihkel Miidla & Liisa Kuuskmaa, *Estonia*, 9 TECH., MEDIA & TELECOM. REV. (2019), https://perma.cc/7Y7V-K9ZR. For an overview of the unique Estonian public-private structure, *see* Anna-Maria Osula, *National Cyber Security Organization: Estonia*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE REPORTS, Tallinn 2015 (the NATO CCDCOE has provided similar helpful reports for many NATO and even some non-NATO states, like Israel).

Parts IV.e. through IV.g. show that unauthorized access, access to restricted data, and even intercepting communications—the sorts of laws most likely to constrain active defense measures—are assigned relatively low maximum sentences in many countries globally. By contrast, in most states surveyed here, "intentional hindrance without right of the functioning of a computer system" (and similar laws using different terms) is the most heavily penalized of the computer crimes. Laws of this type are routinely cited in cases prosecuting perpetrators of denial-of-service attacks.

Every country has such a law and most countries treat the crime more severely than the penalties assigned to other laws examined in the prior sections. Iran,[151] Spain,[152] and Taiwan[153] are the only three exceptions.

<u>Table 5: Interference with normal computer functions</u>

State	**Penalty for interfering with normal computer functions**
Australia	10 years
Canada	10 years
China	5 years; 5-year minimum for serious consequences
Estonia	3–5 years
France	5–7 years
Germany	3–10 years
Iran	6 mo – 2 years
Israel	3–5 years
Japan	3–5 years

[151] *Compare* Majmua-hi Qava-nini Jaza'l [Code of Criminal Laws] Tehran 1388 [2009], articles 734 [9] (interference with normal computer functions punishable by a term of 6 months to 2 years of imprisonment) *with* 733 [8] (unauthorized data destruction punishable by the same term) and 738 [13] (acts committed against critical infrastructure punishable by 3 to 10 years imprisonment). Broadly speaking, Iran has some of the lowest penalties for any computer crimes, unless aggravating factors come into play).

[152] *Compare* CÓDIGO PENAL [C.P.] [Penal Code] art. 264 bis *with* art. 264 (Spain) (interference with normal computer functions and deletion of computer data <u>both</u> punishable by a term of 6 months to 3 years).

[153] *Compare* Zhōnghuá mínguó xíngfǎ (中華民國刑法) [Criminal Code of the Republic of China] 1935, art. 359 *with* art. 360 (Taiwan) (interference with normal computer functions is punishable by a term of 3 years while deletion of computer data is punishable by 5 years).

Netherlands	2–5 years
Oman	2–3 years
Russia	2–5 years
Singapore	5–7 years
South Korea	5 years
Spain	6 mo – 3 years (3–8 years with aggravating factors)
Sweden	6 mo – 6 years
Switzerland	3–5 years
Taiwan	3 years
U.K.	10 years
U.S.	1–20 years *supra* note 135

i. Nuances in laws prohibiting the trade in programs

No survey of computer crime laws could be complete without reviewing how states define and either criminalize or excuse the creation, possession, and trade in programs that enable the previous activities. Here, the Budapest Convention provides a useful framework for looking at different states' laws, both because here states appear to have incorporated some of the particular language of the treaty and because the process of transposing that language into domestic laws exposed fault lines and confusion.

Article 6 is the longest of the substantive computer crime articles in the Budapest Convention. It calls states parties to prohibit the dissemination of devices or computer programs that are "designed or adapted primarily for the purpose of committing" computer crimes and to prohibit the possession of such devices or programs with the intent to commit computer crimes. Importantly, the article goes on to clarify that it "shall not be interpreted as imposing criminal liability" where the dissemination or possession is not for the purpose of committing an offence under the Convention, such as for the authorized testing or protection of a computer system. Under the terms of the

Convention, states parties may reserve the right not to criminalize possession or distribution of these programs, but must in all cases criminalize the trade in passwords and access codes.[154]

As has long been understood, the programs used to commit computer crimes outside one's network (bad, or "black-hat" hacking) are often indistinguishable from programs used to ensure and test internal network security (good, or "white-hat" hacking).[155] Although the complex if-then language of Article 6 explicitly balances the need to prohibit black hat intrusion yet encourage white hat testing, it led to confusion and angst when some Budapest states party transposed it into their domestic laws.

Germany, for example, enacted STGB § 202c in 2007. That section originally provided that

> "Whosoever prepares the commission of an offence under section 202a ["unauthorized access to restricted data at rest] or section 202b [unlawful interception of data in transit] by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible 1. passwords or other security codes enabling access to data…, or 2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.[156]

As enacted, STGB § 202c had no provision clearly exempting research and security testing. Reading the plain language, private sector actors assumed the worst and loudly

[154] *See* Budapest Convention, *supra* note 60, art. 6.

[155] The hat color metaphor is commonly said to derive from old Western films where the "good guys" wore white hats and the "bad guys" black ones, although any number of Internet articles debunk this origin story. Whatever its origins, for one description of current usage *see* Kim Zetter, *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?*, WIRED, Apr. 13, 2016, https://perma.cc/3Y4H-KL87.

[156] STRAFGESETZBUCH [STGB] [Penal Code] § 202c (Ger.). Of note, § 202c was later amended—but not to clarify any of the confusion discussed here. The amendment merely increased the maximum penalty to two years to comply with E.U. Directive 2013/40/EU of Aug. 12, 2013, https://perma.cc/8PWK-6BBP (setting forth guidance—some hortatory, some prescriptive—for member state cybercrime laws). The most interesting point about that E.U. Directive is how although it prompted a number of E.U. members to align their *penalties* as required, few E.U. states made substantive changes to their laws to harmonize with the *hortatory* provisions.

protested. The editors of one outlet even accused the Federal Office for Information Security of violating the law, although the public prosecutor's office dropped the charges.[157] Some cybersecurity companies stopped doing business in Germany;[158] some individuals turned themselves into law enforcement to protest the idea that they could be prosecuted for testing their own network security or distributing tools for network security.[159] Things calmed down after the Federal Constitutional Court ruled that StGB § 202c charges were inadmissible against IT professionals and academics who lacked the requisite intent to use the programs to commit crimes,[160] but the episode lives on as a cautionary tale of how the plain language of laws affects public behavior in rule-of-law cultures.[161]

With the German story as backdrop, Table 6 lays out (1) which states have a prohibition on mere possession of tools that can be used to commit computer crimes, (2) which states only prohibit the trade in such programs, and (3) which states have a formal security research exception or other limiting language.

[157] *See Das BSI und der Hackerparagraf § 202c: Keine Strafverfolgung durch Staatsanwalt [The Federal Office for Information Security and Hacker Paragraph § 202c: Nolle prosequi decision by the prosecutor]*, COMPUTERWOCHE, Oct. 26, 2007, https://perma.cc/JL2J-YBKH (in German).

[158] *See German Security Professionals in the Mist*, SÛNNET BESKERMING COMMENTARY, Aug 12, 2007, https://perma.cc/ER7H-2TR3 (an Australian information security company listing German "security related products and groups [that] have either closed up shop or relocated to countries of convenience, such as the Netherlands").

[159] *See, e.g.*, Daniel Bachfeld, *"Hacker-Paragraf": iX-Chefredakteur zeigt sich selbst an ["Hacker-Paragraph": iX editor-in-chief reports himself]*, HEISE ONLINE, Dec. 19, 2008, https://perma.cc/7EAJ-FMMY (in German).

[160] *See* Bundesverfassungsgericht [BverfG] [Federal Constitutional Court], 2 BvR 2233/07, May 18, 2009, https://perma.cc/6SPL-E6Q5 (in German).

[161] *See, e.g.*, Dennis Jlussi, *Criminalisation of Hacker Tools in German Criminal Law and its Effect on IT Security Professionals*, DENNIS JLUSSI BLOG, Nov. 1, 2007, https://perma.cc/QP8Q-4JAD (a German lawyer summarizing in English a "handle with care – but don't panic" presentation he gave to the 2007 Munich Information Security Summit before StGB § 202c came into effect; also explaining that German law does not criminalize abstract endangerments). As mentioned *supra* note 18, any number of academic articles and public papers have cited to StGB § 202a, Germany's main "hacker" law, presumably because Paul Rosenzweig cited it in a seminal article and it is easy to find and read on the Internet in English translation (not true for every law cited here). No one mentions the far more interesting history of StGB § 202c.

Table 6: Nuances in “hacking tool” laws

State	Possession prohibited?	Trade prohibited?	Penalty?	Research exceptions or other relevant limiting language?
Australia	Yes	Yes	3 years	Only prohibits possession or trade if done “with the intention that the data be used” to commit computer crimes
Canada	Yes	Yes	10 years	Only prohibits possession and trade “without lawful excuse”
China	Creation prohibited; possession not prohibited	Yes	3–7 years	Only prohibits actual use or trade with knowledge of what it will be used for; or creation of programs that by their nature have a destructive purpose (e.g., certain viruses)
Estonia	Yes	Yes	2 years	Only prohibits programs designed “in particular for the commission of” computer crimes.
France	Yes	Yes	5–7 years	Only prohibits programs “specially adapted” to commit computer crimes Research or computer security is an explicit exception
Germany	Yes	Yes	2 years	The Constitutional Court has treated the phrase “for the purpose of” as incorporating a specific intent element
Iran	No	Yes	91 days – 1 year	Only prohibits trade in programs “exclusively used” to commit computer crimes
Israel	Creation prohibited; possession not prohibited	Yes	3–5 years	Prohibits trade in all programs “enable[d] to perform” computer crimes
Japan	Yes	Yes	2–3 years	Only prohibits possession and trade “without just reasons” of programs that “cause the computer to be operated against the operator’s intention or to fail to be operated in accordance with the operator’s intention.”
Netherlands	Yes	Yes	3–5 years	Only prohibits possession or trade in programs “with the intention of using it in the commission of a serious offence”
Oman	Yes	Yes	6 mo – 3 years	Only prohibits trade in programs designed for the purpose of committing computer crimes; only prohibits possession with an intent to use the program in committing computer crimes

Russia	Creation prohibited; possession not prohibited	Yes	4–7 years	Only prohibits creation/trade of programs “knowingly intended for” use in committing computer crimes
Singapore	Yes	Yes	3–5 years	Only prohibits possession or trade in a program when “intending to use it to commit, or facilitate the commission of” a computer crime
South Korea	No	Yes	7 years	Only prohibits trade in programs “likely to interrupt operation” of a computer system
Spain	No	Yes	6 mo – 2 years	Only prohibits trade in programs with the intention to facilitate computer crime
Sweden	Only prohibited if done as a preparatory act[162]		2 years	Neither possession nor trade is prohibited, *unless* done in preparation for a data breach
Switzerland	Creation prohibited; possession not prohibited	Yes	3 years	Only prohibits creation or trade in programs which one “knows or must assume are intended to be used to commit a” computer crime.
Taiwan	Creation prohibited; possession not prohibited	Prohibits creating programs for another	5 years	Only prohibits creation or trade in programs when done “specifically for himself or another to commit” a computer crime
U.K.	Creation prohibited; possession not prohibited	Yes	2 years	Prohibits creation of programs intended for use in committing computer crimes; Prohibits trade in programs believing they are likely to be used to commit computer crimes
U.S.	Creation prohibited; possession of > 15 programs with intent to defraud also prohibited	Yes	10–20 years	Intent element: “knowingly and with intent to defraud” In addition, computer code in the U.S. enjoys some degree of protection under the First Amendment to the U.S. Constitution.[163]

[162] *See* Anders Hellström & Erik Myrberg, *Sweden: Cybersecurity 2019*, INTERNATIONAL COMPARATIVE LAW GUIDE, Oct. 16, 2018, https://perma.cc/9GNJ-FW5N (citing an unspecified Swedish Court of Appeal).

[163] *See, e.g.*, Bernstein v. United States Department of State, 922 F. Supp. 1426 (N.D.C.A. 1997) and its subsequent and convoluted appellate history; *see also* Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

The takeaways are straightforward:

(1) Nine states prohibit the possession of programs that can be used to commit computer crimes, while seven states (China, Israel, Russia, Switzerland, Taiwan, the U.K., and the U.S.) prohibit creating such programs "with intent to commit computer crimes" or similar language but don't prohibit possession per se. Three states (Iran, South Korea, and Spain) don't prohibit possession at all, merely use and trade. Sweden is in a category of its own, prohibiting neither possession nor trade per se.

Perhaps unsurprisingly, this puts the states widely believed to have significant military or other public sector cyber powers (i.e., China, Iran, Israel, Russia, the U.K., and the U.S.) on the "more permissive" end of the spectrum.

(2) By contrast, every state restricts the trade in such programs. And every state assigns the crime of trade in programs a relatively serious maximum possible penalty.

(3) Japan is unique for its narrow focus only on programs that "cause the computer to be operated against the operator's intention or to fail to be operated in accordance with the operator's intention."[164] Japan has no clear law prohibiting possession or trade in programs that would enable, e.g., unauthorized access to data at rest or interception of data, *if* that access or interception doesn't interfere with the normal operator's ability to access the data.

(4) Every state surveyed has some form of language (or case law clarifying the statutory language, in the case of Germany) that makes the prohibited possession or trade in such programs only criminal if done with intent to commit or facilitate an unlawful act. In a sense, this intent language implies a sphere of lawful activity.

[164] Hayashi, *supra* note 102. *See also supra* note 86 and KEIHŌ (PEN. C.) 1907, art. 168-2 (Japan).

(5) Yet no state except France has an explicit exception for programs used for research and security testing.[165] This does not necessarily mean that research and security testing will be prosecuted. For example, the U.S. does not have a formal security research exception, but the DoJ told the 2015 Black Hat conference that average sentences for CFAA violations have "routinely been below the minimum Guideline sentence that could be imposed" and "In comparison to other federal crimes, CFAA offenses are not charged frequently – and prosecuting someone engaged [sic] computer security research is extraordinarily rare." [Underscores in original.][166] Still, as the German example suggests, where the law facially prohibits such programs and cybersecurity professionals must rely on prosecutorial discretion rather than an explicit legal defense, the overall effect can be chilling.

Taken together, this suggests that it is not by chance that, at least according to one ranking, the most innovative cybersecurity companies in the world are clustered in a handful of states, of which all but Canada are clearly relatively permissive in their official

[165] CODE PÉNAL [C. PÉN.] [Penal Code] art. 323-3-1 (Fr.). *See also* CODE DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES [Post and Electronic Communications Code], arts. 33-14 & 34-1 (Fr.). Of note, France only added this "research or computer security" exception in 2013. *See* Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law 2013-1168 of December 18, 2013 on military programming for the years 2014 to 2019 and containing various provisions concerning defense and national security], art. 25, Dec. 20, 2018, https://perma.cc/L38C-NV8A.

[166] *See* Presentation by Leonard Bailey, Special Counsel for National Security, U.S. Department of Justice Computer Crime and Intellectual Property Section (Aug. 5, 2015) https://perma.cc/2F2T-XVDZ. In FY2017, for example, 165 cases were filed in which a CFAA violation was listed. U.S. Attorneys' Annual Statistical Report Fiscal Year 2017, Table 3B, https://perma.cc/FJ9N-XE67. To focus on a particular example from 2013–2014, *see also* Jordan Robertson & Michael Riley, *Would the U.S. Really Crack Down on Companies that Hack Back?*, BLOOMBERG, Dec. 30, 2014, https://www.bloomberg.com/news/2014-12-30/why-would-the-u-s-crack-down-on-companies-that-hack-back-.html and Michael Riley & Jordan Robertson, *FBI Probes If Banks Hacked Back as Firms Mull Offensives*, BLOOMBERG, Dec. 30, 2014, https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives (both articles suggesting that the FBI was investigating U.S. banks for taking aggressive active defense measures, but that the DoJ was unlikely to bring charges due to the fragility and importance of public/private sector relations in the cybersecurity sphere).

attitudes towards the possession of computer programs: the U.S., Israel, the U.K., Canada, France, Sweden, and China.[167]

j. Other relevant laws:

Finally, we examine other laws that might be relevant to private sector actors trying to conduct active defense measures. Here we find a variety of approaches, mostly regarding the treatment and powers of internet service providers (ISPs).

States commonly have an exception in their relevant interception law that permits an ISP to monitor its networks as needed for basic quality of service.[168] Notably, Australia, Canada, and China also permit ISPs (but not other companies) to take affirmative protective measures on their own.

Specifically, Australia permits an ISP to trace any person "suspected of a violation" of the computer crimes discussed here.[169] Canada similarly authorizes ISPs to intercept communications "if the interception is reasonably necessary for… protecting the computer system against any act that would be an offence under [the computer crimes

[167] *See supra* note 76. Why Canada, with its consistently strict penalties and broad prohibitions, has so many cybersecurity companies is a good question for future research.

[168] Even the United States. *See* 18 U.S.C. § 3121(b) and 18 U.S.C. § 2511(1)(h).

[169] "[The general interception prohibition] does not apply to or in relation to: (a) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:…(iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the Criminal Code [computer crimes]; where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or…(aaa) the interception of a communication by a person if: (i) the person is authorised, in writing, by a responsible person for a computer network to engage in network protection duties in relation to the network; and (ii) it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively…" *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 ss 7(2)(a) & (aaa) (Austl.).

discussed here].”[170] China criminalizes an ISP’s failure to protect its network if it fails to comply with basic security requirements (to be defined by regulation).[171]

By slight contrast, France permits ISPs to use devices on their networks to detect events likely to affect the security of the network—but only under state supervision.[172] In Estonia,[173] and South Korea, [174] ISPs are required to monitor their networks (but not authorized to intercept the content of communications except as required for quality of service) and then hand off any information that suggests adverse cyber activity to the state. In Estonia,[175] Singapore,[176] and South Korea,[177] the state has the power to direct

[170] “Saving provision: (2) [the general interception prohibition] does not apply to… (e) a person, or any person acting on their behalf, in possession or control of a computer system…who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for… (ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) [unauthorized access] or 430(1.1) [modifying data]. Canada Criminal Code, R.S.C. 1985, c C-46, art. 184(2)(e) (Can.).

[171] Zhonghua Renmin Gongheguo Xingfa (中华人民共和国刑法) [Criminal Law of the People’s Republic of China] (promulgated by the Fifth National People’s Congress on July 1, 1979) (ninth amendment promulgated by the Standing Committee of the Second National People’s Congress on Aug. 29, 2015, effective Nov. 1, 2015), art. 286 (China).

[172] “For the purpose of security and defense of information systems, electronic communications operators may use, on the electronic communications networks they operate, after informing the national security authority of the information systems, to devices implementing technical markers solely for the purpose of detecting events likely to affect the security of the information systems of their subscribers.” CODE DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES [Post and Electronic Communications Code], arts. 33-14 & 34-1 (Fr.) [emphasis added].

[173] KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018, c. 2 § 7 (Est.).

[174] “A person falling under any of the following subparagraphs shall furnish the [state] with the information related to intrusion cases, including statistics by type of intrusion cases, statistics of traffic of the relevant information and communications network, and statistics of use by access channel, as prescribed by Presidential Decree:

1. A major provider of information and communications services;
2. A business operator of clustered information and communications facilities;
3. Other persons specified by Presidential Decree among those who operate an information and communications network.” Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. [commonly known as the Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, art. 48-2, *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.).

[175] KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018, c. 4 (Est.).

[176] *See supra* note 97.

[177] “The [state] may, if necessary to take countermeasures against intrusion, request [that ISPs] provide human resources for assistance.” Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. [commonly known as the Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, art. 48-2(6), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.).

the ISP's defenses. By contrast, ISPs in Japan are required by law to restrict their response to basic public-private information sharing.[178]

With the exception of the draft laws in the U.S. and Israel already discussed, states are generally silent on active defense authorities outside the limited exception for ISPs. But they can and do prohibit computer crimes when carried out under the authority of a group or corporation. Unsurprisingly, every state surveyed has some general provision pertaining to corporate liability in its penal or procedural code.[179]

Table 7: Other relevant laws

State	Any other laws relevant to active defense measures?
Australia	Telecommunications Act § 7 permits ISPs to trace any person suspected of any provision of Part 10.6 of the Criminal Code (i.e., all computer crimes relevant here). The state can take various measures under the Surveillance Devices Act 2004 and similar laws.
Canada	Criminal Code § 184(2)(e) exempts from the prohibition on intercepting communications any person in possession or control of a computer system, "who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for…(ii) protecting the computer system against any act that would be an offence under [all computer crimes discussed here]".
China	Article 286 criminalizes network service providers' failure to protect their networks if they don't comply with basic security requirements (to be defined by regulation) and the failure results in a serious situation (e.g., large personal information data leaks).
Estonia	The Cybersecurity Act requires that ISPs monitor their networks but reserves any out-of-network active defense measures to the state or ISPs working under state supervision.

[178] Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, arts. 8–10 (Japan), (encouraging ISPs and network administrators to harden internal network defenses and public-private information sharing).

[179] *C.f.* Budapest Convention, *supra* note 60, art. 12 (calling states parties to establish provisions for corporate liability). Here, too, there is no obvious distinction in either substance or organization between the laws of Budapest states parties and non-states parties.

France	The Internal Security Code Article L853-2 governs state hacking. The Code des postes et des communications électronique, Articles L33-14 and L34-1, permits ISPs to use devices on their networks to detect events likely to affect the security of the network—under state supervision.
Germany	Security testing is permitted in practice.
Iran	None known.
Israel	None currently known. *But contemplated. See Part IV.d.(3) supra.*
Japan	UCAL Arts. 8–10 encourage ISPs and network administrators to harden internal network defenses and public-private information sharing.
Netherlands	Computer Crime Act III provides a legal framework for state (police) hack-back, but not for private sector actors.
Oman	None internal to the Cyber Crime Law.
Russia	None known.
Singapore	Cybersecurity Act § 23 permits the state to direct ISPs conducting interception measures.
South Korea	Network Act Article 48-2 governs state supervision of ISPs conducting countermeasures to protect against intrusion. The law permits those countermeasures to be defined by Presidential Decree rather than by law. Infrastructure Protection Act Art. 13 requires private-public information sharing and authorizes the government to take “necessary measures” to prevent the spread of damage and “swiftly respond.”
Spain	Penal Code Arts. 31 bis, 33, 197 quinquies and 264 quater lay out an extensive commentary on how corporate liability is assigned.
Sweden	None known.
Switzerland	None known.
Taiwan	The Communication Security and Surveillance Act reserves all cyber intrusion and surveillance activity to the state through a warrant process. ISPs may be ordered to act at the direction of the state upon a warrant.
U.K.	The Investigatory Powers Act reserves all cyber intrusion and surveillance activity to the state through a warrant process. No authorization for ISPs to act in self-defense of networks.
U.S.	*Contemplated. See Part IV.d.(3) supra.*

V. CONCLUSION:

Throughout this paper I've focused on simple description rather than on big normative theories; the normative space is crowded and the descriptive space relatively unoccupied. This asymmetry is strange, as the law on the books provides essential groundwork for the normative arguments—perhaps even more so if, as some argue, the law on the books doesn't always reflect reality. How can we know what ideas are worth exploring if we don't know what the law says, what is common, and what is rare?

In this Part, I draw some very basic conclusions from what I've described above and ask what this means for the future of the U.S.-based discussion around active defense measures. From what I've described above, what is fair to paint broadly?

First, that states tend to criminalize the same sorts of private activity in cyberspace: access to data at rest; modifying data at rest; intercepting data in transit; and hindering normal computer functions. Although each may phrase its laws differently, no country surveyed here has found a "new" type of crime or an "obviously" better way to identify conduct that should be prohibited. Cyberspace is not a lawless "Wild West."[180] Rather, it is teeming with law—and with few exceptions, that law isn't especially hard to find and is broadly similar across jurisdictions.

Rosenzweig argued in 2014 that "other nations have generally not considered the concept of private-sector self-defense. Rather, their attitude must be inferred (if it can be inferred at all) from their silence."[181] But when we look around today, we find very little silence. U.S. private sector actors should indeed be cautious of taking action that could

[180] Not a new point, but an underscore for emphasis. *See also* Joseph S. Nye, Jr., *Cyber Power*, BELFER CENTER ESSAY (2010) at 14, https://perma.cc/8CXC-C6BZ.
[181] Rosenzweig, *supra* note 13 at 114.

affect servers or data over which other countries have jurisdiction, because if this initial survey is any representative guide, many countries with significant Internet infrastructure will have laws that restrict private sector activity much like the U.S. does. As Rosenzweig reasonably points out, although the U.S. is unlikely ever to extradite a U.S. person to an adversary state, the U.S. would have a harder time dismissing an appropriately couched extradition request from, say, Germany, Japan, Taiwan, or Israel.[182] And there is no reason to believe that the passage of time will thin out rather than thicken these laws around the world.

Second, although among these twenty states there is no jurisdiction that is officially or overtly permissive, some are relatively permissive, either because they choose not to criminalize an activity based on a substantive distinction or because they assign lower penalties to such crimes. For example, eight of the twenty states surveyed do not bar mere access to data at rest. Six more do, but have relatively low maximum penalties (i.e., two years or less). Only six states, including the U.S., bar unauthorized access to unprotected data at rest. Interestingly, Iran, Oman, and Spain consistently assign low-level penalties to low-level computer crimes across the board.[183] But it would be wrong to think of those last three states as fundamentally permissive jurisdictions; in fact, when aggravating factors are present, their laws assign penalties just as high as other states. Rather, we might reason that those states (among the fourteen mentioned above) simply wish to make clear in their laws what types of activity are important and which are not. By contrast, a common criticism of the U.S. CFAA is that it is *particularly unclear* in its text about what is important and what is not.

[182] *See* Rosenzweig, *supra* note 13 at 115.
[183] *See supra* Tables 2–5.

Third and by contrast, Canada, China, South Korea, and the U.S. have clearly and consistently higher penalties on the books than other states. Yet we know, for example, that the U.S. DoJ has told hacker conferences that they are unlikely to pursue low-level crimes (definition unclear) or security researchers. In addition, we know that some significant portion of the cybersecurity companies of the world have clustered in these countries, despite how strict their laws appear. How can we explain this? One logical question for future research would look more deeply at whether "official disapproval with informal tolerance" is indeed becoming the "recurring model across the globe," or at least in those countries with relatively high potential penalties for computer crimes.[184]

Fourth, mapping out the landscape this way brings into relief interesting details that are otherwise hard to see. Of the states surveyed here, Australia's laws are by far the most detailed, lengthy, and granular; Sweden's are shortest. They both cover the same ground. Japan's laws are the most different from other states, especially in how they focus on protecting specific types of data that affect property and legal rights, rather than on some inchoate concept like protecting data for its own sake. We find surprising oddities, like France and Japan's decision to penalize intercepting data in transit less severely than accessing data at rest, or Estonia's decision to constitutionalize communications privacy but punish violations with just a fine. This overview can't always explain why these differences exist—some will be for detailed historical reasons, some by chance—but mapping out these laws side by side at least allows us to see where the differences *are* and ask, as a policy matter, which ideas might be worth exploring further.

[184] *Id.* at 115.

And fifth, we see overall just how rare it is for a country to contemplate loosening rules for private sector active defense measures. That's not to say that the U.S. shouldn't do something just because it would be an outlier—the U.S. is often an outlier. It is, however, a fair to question to ask how useful it would be to loosen U.S. law, given the international thicket that has grown up in domestic laws globally.

What does this mean for the future of the U.S.-based discussion around active defense measures? Broadly, that *all* of the prevailing voices would benefit from looking outside our borders when formulating their arguments. Those arguing for aggressive offense by both private and public sectors;[185] for a more measured set of private sector active defenses;[186] for abandonment of the "active defense" model in favor of other more productive models for acting on intelligence sharing;[187] for careful vetting of companies authorized to take certain active defense measures under the supervision of the U.S. government;[188] for caution given that the more oversight the government exercises over the private sector the more likely state responsibility doctrine is to apply;[189] for a polycentric model[190]—and so on—all of these voices would do well to remember Rosenzweig's 2014 call for a better understanding of the domestic laws of other countries. We're not there yet; this paper provides a baseline for and the sketch of a map towards that better understanding.

[185] *See* Baker, *The Hackback Debate*, *supra* note 10 and Stewart Baker, *Four principles to guide the US response to cyberattacks*, FIFTH DOMAIN, Feb. 7, 2019, https://perma.cc/82V2-S6F8.
[186] *See*, *e.g.*, CCHS Report, *supra* note 14.
[187] *See*, *e.g.*, Cook, *supra* note 26.
[188] *See*, *e.g.*, Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up*, HOOVER WORKING GROUP ON NAT. SEC. TECH. & L., AEGIS SERIES PAPER NO. 1606 (Jun. 22, 2016) at 15–16, https://perma.cc/8VKT-MRY8.
[189] *See*, *e.g.*, Kristen Eichensher, *Would the United States Be Responsible for Private Hacking?*, JUST SECURITY, Oct. 17, 2017, https://perma.cc/HL5U-P9R7.
[190] *See*, *e.g.*, the articles by Shackelford *et al*, *supra* note 19.

APPENDIX—REVELANT DOMESTIC LAWS

Following each state's long-form name, I include a Bluebook (20th ed.) citation for the relevant laws cited in the essay.

For states whose governments publish the laws in up-to-date English (original or translation) online, I provide a permalink to that version. Where the translation source is obvious from the permalink, I generally do not note the translator except when directed by the Bluebook (i.e., Japan, South Korea).

For states whose government-provided English translations are out of date, I provide a permalink to the most recent English version provided, note relevant amendments up to April 2019, and provide a permalink to the current law in the original language.

For states whose governments do not publish English translations online, I provide permalinks to the most reputable up-to-date source I could find.

For China, Iran, Israel, and Russia, I have linked to versions hosted by reputable non-governmental or inter-governmental organizations (such as the UNODC or WIPO) whose websites are more easily accessible for many U.S. readers.

One Israeli law, two Japanese articles, and one Russian article are not readily available in English on the Internet; because of the difficulty involved in finding them, I have copied the relevant text here. The Hebrew and Japanese translations are from official sources; the Russian is mine, with initial assistance from Google Translate. Two French laws and one Spanish law are not available in English online, but I trust that English-speaking readers can either use an online translation service or locate translators relatively easily.

[The Commonwealth of] Australia

Criminal Code Act 1995 (Cth) ch 10 pt 6 (Austl.), https://perma.cc/L2H4-3ETP .

Telecommunications (Interception and Access) Act 1979 (Cth) ch 2 (Austl.), https://perma.cc/N7TB-PEJM.

Canada

Canada Criminal Code, R.S.C. 1985, c C-46 (Can.), https://perma.cc/Z2EE-V3XS.

[The People's Republic of] China

Zhonghua Renmin Gongheguo Xingfa (中华人民共和国刑法) [Criminal Law of the People's Republic of China] (promulgated by the Fifth National People's Congress on July 1,

1979) (ninth amendment promulgated by the Standing Committee of the Second National People's Congress on Aug. 29, 2015, effective Nov. 1, 2015), arts. 283–287 (China).

- The most recent English translation includes only Amendments 1–8: https://perma.cc/UQT8-7BMW. The 9th Amendment (2015) amended: (1) Articles 283–286 to make clear that corporations who violate those articles are liable for fines and those within the corporation responsible for the violation are criminally responsible for the respective penal provisions; (2) Article 286 to criminalize network service providers' failure to comply with security requirements set forth by law and regulation, if the failure results in a serious situation (e.g., personal user information data leaks or large transmissions of other illegal information); and (3) Article 287 (also inserting Article 287bis) to criminalize knowing provision of technical support (such as providing hacking tools) or material support (such as providing server space, Internet access, etc.) to online criminals, https://perma.cc/DT7C-NRUR. *See also* Jeremy Daum, *It's a crime, I tell ya: Major Changes in China's Criminal Law Amendment 9*, CHINA LAW TRANSLATE BLOG, Sep. 27, 2015, https://perma.cc/4P2T-B5UB.

[The Republic of] Estonia

- Of note, Estonian sections sometimes include superscript characters—these are not to be confused with footnotes, but refer instead to code sections inserted between pre-existing numbers.

EESTI VABARIIGI PÕHISEADUS (Constitution of the Republic of Estonia) 1992, https://perma.cc/J3YF-PC99.

KARISTUSSEADUSTIK (Penal Code), c. 13 (Est.), https://perma.cc/6H6W-EHDK.

ELEKTROONILISE SIDE SEADUS (Electronic Communications Act) 2005, c. 10 (Est.), https://perma.cc/C3P3-NQUL.

KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018 (Est.), https://perma.cc/YY2H-UQ2A.

France [The French Republic]

- Of note, French articles use hyphens to indicate subparagraphs or sub-articles. These are not to be confused with numerical ranges marked by en-dashes.

CODE PÉNAL [C. PÉN.] [Penal Code] art. 323 (Fr.).

- The most recent English translation is from 2005, https://perma.cc/P96C-WY3H. Amendments since 2005 increased the fines throughout this article, added the paragraphs increasing the penalties for crimes committed against state computers, added several verbs to the list in article 323-3, added the "research or computer security" exception to article 323-3-1, and added article 323-4-1, https://perma.cc/6LW8-GRZV.

CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [Criminal Procedure Code], art. 706-102 (Fr.), https://perma.cc/HYG6-YJZ7 (procedures governing state oversight of interception).

CODE DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES [Post and Electronic Communications Code], arts. 33-14 & 34-1 (Fr.), https://perma.cc/Y2KX-A7ED and https://perma.cc/52QM-WR84 (governing exceptions to art. 323 of the Penal Code).

[The Federal Republic of] Germany

STRAFGESETZBUCH [STGB] [Penal Code] (Ger.).

- The most recent English translation is from 2013, https://perma.cc/9ZVR-X4LJ. Amendments since 2013 increased the penalty in § 202c and added subparagraph (3) to § 303a, https://perma.cc/EYQ3-X6MK.

[The Islamic Republic of] Iran

MAJMUAHI QAVAINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1381 [2002], arts. 726–750 [corresponding to Computer Crime Act 1388 [2009] arts. 1–25] (Iran).

- The Computer Crime Act is available in up-to-date English translation at https://perma.cc/8SJK-XSGG. *See also* cyber.police.ir. Although Article 55 of the Computer Crime Act states that "Articles (1) to (54) of the present act are considered as Articles (726) to (782)" of the Code of Criminal Laws, the Code has not yet been revised to reflect this. For citation purposes in this essay, I provide both the Code number [and the Act number following in brackets].

[The State of] Israel

Computers Law 5755-1995, A.G. Pub., 2015 (Isr.).

- The Computers Law has yet to be codified into the Laws of the State of Israel (LSI). In this essay, I have used a 2015 translation from Aryeh Greenfield Publications (reputable but unofficial), which incorporates the 2012 amendments that Israel made to harmonize the law with the Budapest Convention.

- The A.G. Pub. version is not available online. Another translation accessible online that generally matches the A.G. Pub. translation can be found at https://perma.cc/N9LK-Q9E6 (but as this version does not include citation or translation information, I did not use it in this essay).

Wiretap (Secret Monitoring) Law 5739-1979, 33 LSI 141 (Isr.).

- I found no Internet source for this law in English, although the law itself is publicly available in LSI hard copy. The official translation provides in relevant part that

> 1. In this Law ¬…"monitoring" means listening to the conversation of another by means of an instrument; … "secret monitoring" means monitoring without the consent of any of the participants in the conversation and includes the recording thereof; … "conversation" means conversations by word of mouth or by any other means of communication;…
>
> 2. (a) A person who without a proper permit engages in secret monitoring shall be liable to imprisonment for a term of three years. (b) A person who knowingly, without lawful authority, uses any information, or the contents of any conversation, obtained by secret monitoring, whether authorised or unauthorised, or knowingly discloses any such information, or the contents of any such conversation, to a person not competent to receive it shall be liable to imprisonment for a term of three years. (c) A person who sets up or installs an instrument for the purpose of unauthorised secret monitoring or to enable the use thereof for that purpose shall be liable to imprisonment for a term of one year.

Japan

KEIHŌ (PEN. C.) 1907, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan).

- The most recent English translation available online is up-to-date but contains two errors, https://perma.cc/4RNP-FL46. As discussed *supra* note 86, Articles 168-2 and 168-3 were added to the Penal Code by Amendment June 24, 2011 (and are clearly mentioned in Japan's 2012 reservations to the Budapest Convention), but have yet to appear on https://www.japaneselawtranslation.go.jp. I've transcribed [sic] the translation of those two articles below from the EHS Law Bulletin Series II (PA 37) 2011.

- Article 168-2

    - 1. The person who has prepared or has provided the electromagnetic records and other records mentioned in the following for the purpose of providing for the use of operation of computers of people without just reasons shall be punished with penal servitude for not more than three years or a fine not more than five hundred thousand yen:

      (1) The electromagnetic records that give unjust directive not to work to follow his/her intention when people use computers or to go against his/her intention [i.e., hindering normal computer functions];

      (2) In addition to those mentioned in the preceding item, electromagnetic records or other records describing unjust directive under the said item.

    - 2. The same shall apply as the preceding paragraph to the person who provides the electromagnetic records mentioned item (1) of the preceding paragraph for the use of operation of computers of people without just reasons [i.e., trade in programs that hinder normal computer functions].

    - 3. The attempted of the crimes under the preceding paragraph shall be punished.

- Article 168-3 (Obtaining, etc., of unjust electromagnetic records) [obtaining or retaining for future use programs adapted for computer crimes]

    - The person who obtained or kept the electromagnetic records and other records mentioned in the respective items of paragraph 1 of the preceding Article for the purpose of paragraph 1 of the preceding Article without just reasons shall be punished with penal servitude for not more than two years or a fine not more than three hundred thousand yen.

Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan), https://perma.cc/MLY2-9KSA.

Denki tsūshin jigyō-hō [Telecommunications Business Act] Act No. 86 of 1984, *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan), https://perma.cc/28FF-PSYC.

[Kingdom of the] Netherlands

Wetboek van Strafrecht [SR] [Criminal Code] (Neth.).

- The most recent English translation is from 2012, https://perma.cc/MR69-E6SJ. Amendments since 2012 increased the penalties in Sections 139c and 139d, eliminated one of the subparagraphs in Section 161sexies, and added subparagraphs 2–5 to Section 138b, Wetboek van Strafrecht.

- The Computer Crime Act III (effective March 2019) provides a legal framework for state (police) hacking, but does not otherwise substantively change the articles relevant in this essay. *See* https://perma.cc/DL7K-HYFN (in Dutch).

[Sultanate of] Oman

Royal Decree No. 12, Feb. 6, 2011, Issuing the Cyber Crime Law (Oman), https://perma.cc/ZK5V-Z83Z.

Russia [Russian Federation]

UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] (Russ.).

- English translations of the Russian Criminal Code are rare. One relatively recent (2012) English translation is hosted by the World Intellectual Property Organization (WIPO), https://perma.cc/TF3D-TSAA.

- Key amendments since 2012 include the addition of article 159.6 (theft of another's property or the acquisition of the right to another's property by entering, deleting, blocking, modifying computer information or otherwise interfering in the operation of means of storing, processing or transmitting computer information or information and telecommunication networks) and increased fines in article 272, https://perma.cc/EV7K-XBE4 (Russian text in rtf format hosted by the UNODC, downloaded in 2018 from consultant.ru, a Russian database akin to Lexis or Westlaw).

- As article 159.6 is not readily available in English, I've provided an unofficial translation here:

    - 1. Fraud in the field of computer information, that is, theft of another's property or the acquisition of the right to another's property by entering, deleting, blocking, modifying computer information or otherwise interfering in the operation of means of storing, processing or transmitting computer information or information and telecommunication networks –

shall be punished with a fine of up to one hundred twenty thousand rubles or in the amount of the salary or other income of the convicted person for a period of up to one year, or compulsory work for up to three hundred and sixty hours, or correctional work for up to one year, or restriction of freedom for up to two years, or forced labor for up to two years, or arrest for up to four months.

- 2. The same act committed by a group of persons in a preliminary conspiracy, as well as causing significant damage to a citizen –

  shall be punished with a fine of up to three hundred thousand rubles or in the amount of the salary or other income of the convicted person for a period of up to two years, or compulsory work for up to four hundred and eighty hours, or correctional work for up to two years, or forced labor for up to five years with restriction of liberty for up to one year or without it, or imprisonment for up to five years with restriction of liberty for a period of up to one year or without it.

- 3. The acts provided for in the first or second part of this article, committed:
  - a) by a person using his official position;
  - b) on a large scale; [or]
  - c) from a bank account, as well as in relation to electronic funds, -

  shall be punished with a fine in the amount of from one hundred thousand to five hundred thousand rubles or in the amount of the salary or other income of the convicted person for a period of one to three years, or forced labor for up to five years with restraint of liberty for a term of up to two years or without imprisonment for up to six years with a fine of up to eighty thousand rubles, or in the amount of the salary or other income of the convicted person for a period of up to six months or without it and with restriction of freedom for up to one and a half years or not.

- 4. The acts provided for in the first, second or third part of this article, when committed by an organized group or on a large scale –

> shall be punished with imprisonment for up to ten years with a fine of up to one million rubles or in the amount of the salary or other income of the convict for a period of up to three years or without such and with restriction of freedom for up to two years or without it.

[Republic of] Singapore

Computer Misuse Act 1993, c. 50A § 1–9 (Sing.), https://perma.cc/4WGF-9Y58.

Cybersecurity Act 2018, § 23 (Sing.), https://perma.cc/XKC6-3US9.

South Korea [Republic of Korea]

Criminal Act, Act No. 293, Sep. 18, 1953, *amended by* Act No. 14415, Dec. 20, 2016, *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.), https://perma.cc/WDV4-R7YJ (not cited in the essay, but includes a few prohibitions on business fraud, etc., not covered in the following two acts).

Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. [commonly known as the Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.), https://perma.cc/F6RD-MEUM.

Act on the Protection of Information and Communications Infrastructure, Act No. 6383, Jan. 26, 2001, *amended by* Act No. 14839, Jul. 26, 2019, *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do (S. Kor.), https://perma.cc/9EN9-3JB8.

[Kingdom of] Spain

CÓDIGO PENAL [C.P.] [Penal Code] (Spain), https://perma.cc/YBX7-93G3.

[Kingdom of] Sweden

BROTTSBALKEN [BrB] [PENAL CODE] 4:8–9c (Swed.).

- The most recent English translation is from 1999, https://perma.cc/7SBA-AYJD. Amendments since 1999: (1) made a minor change to the phrasing of 4:8; (2) inserted a cross-reference to 4:6a into 4:9b; and (3) added additional penalties to 4:9c for “serious” intrusions, https://perma.cc/VEM6-MZS6.

Switzerland [Swiss Confederation]

SCHWEIZERISCHES STRAFGESETZBUCH [STGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757, arts. 143–147 (Switz.), https://perma.cc/PVU8-YHXD.

Taiwan [Republic of China]

Zhōnghuá mínguó xíngfǎ (中華民國刑法) [Criminal Code of the Republic of China] 1935, arts. 358–362, *translated in* Laws & Regulations Database of The Republic of China, https://law.moj.gov.tw/Eng/index.aspx (Taiwan), https://perma.cc/M8H6-QS5K.

Tōngxùn bǎozhàng jí jiānchá fǎ (通訊保障及監察法) [The Communication Security and Surveillance Act] 1999, art. 24, *translated in* Laws & Regulations Database of The Republic of China, https://law.moj.gov.tw/Eng/index.aspx (Taiwan), https://perma.cc/TNS2-NP6W.

U.K. [United Kingdom of Great Britain and Northern Ireland]

Computer Misuse Act 1990, c. 18, §§ 1–3 (UK), https://perma.cc/5V2W-R2DV.

Investigatory Powers Act 2016, c. 25, § 3 (UK), https://perma.cc/X8AA-X57L.

U.S. [United States of America]

18 U.S.C. § 1030 (the Computer Fraud and Abuse Act (CFAA))

18 U.S.C. § 2510 *et seq*. (the Wiretap Act)

18 U.S.C. § 3121 (the prohibition on pen register/trap and trace devices)