# ARTICLE

## A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace

Brian Corcoran*

* Lieutenant Commander, Judge Advocate General's Corps, U.S. Navy. LL.M., 2019, Harvard Law School; J.D., 2009, Geo. Univ. Law Center; A.B., 2006, Brown Univ. This article began life as a research paper submitted in partial fulfillment of the requirements of a Master of Laws degree at Harvard Law School, funded through the Naval Postgraduate School's civilian education program, and may be available in an earlier form at DTIC.mil. The views expressed here are the author's and do not reflect the official policy or position of the Department of the Navy, Department of Defense, or the U.S. Government. This article has been cleared for public release through a U.S. Navy pre-publication security review. My thanks to Jack Goldsmith, Jane Bestor, and the staff of the Harvard National Security Journal for helpful comments and feedback and to the Harvard Law Library and to Stephen Wiles for research assistance; any errors are, of course, my own.

Abstract

The U.S. private sector is vulnerable in cyberspace. In response, an increasingly mainstream national security argument calls for amending U.S. law to permit private sector actors to employ so-called "active defense" measures—a group of loosely-defined technical measures that fall on a spectrum between passive firewalls (clearly legal) and offensive counterattacks (clearly illegal). Proponents argue that such measures could slow, identify, or even deter offenders in cyberspace; provide unclassified evidence for use in civil cases; or support a government response. Critics warn of careless or incompetent actors and second-order effects—of companies starting a war.

Strikingly, the U.S. debate over active defense measures is missing a comparative view of the rest of the world. There are no answers to straightforward descriptive questions, such as, "are active defense measures illegal (or otherwise constrained) in other countries?"

This Article is the first sizable study to answer some of those basic comparative questions. It surveys the laws of twenty countries, (1) finding a remarkable uniformity of approaches that, while not yet rising to the standard of an international norm or custom, is closer than most assume and (2) concluding that even if Congress relaxes U.S. law to permit certain private sector active defense measures, laws around the world will continue to constrain private sector activity.

**Table of Contents**

"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."[1]

— Microsoft President Brad Smith

"[Y]ou can't have companies starting a war."[2]

— General (retired) Keith Alexander, former U.S. National Security Agency director

## I. Background

### A. *The Situation*

The United States government, for all its vast public sector national security resources, has struggled with how best to protect its massive but vulnerable private sector from malign foreign state activity in cyberspace. The number of known or suspected state-linked cyber activities targeting private individuals and corporations continues to grow,[3] while the U.S. government cannot defend the private sector everywhere at all times due to resource constraints, fear of escalating conflict, and domestic norms.[4]

Public international law and norms provide little if any guidance on how a state can or should respond to another state's cyber activity targeting its private

---

[1] Steve Ranger, *Why Microsoft is Fighting to Stop a Cyber World War*, ZDNET (Dec. 12, 2018), https://www.zdnet.com/article/why-microsoft-is-fighting-to-stop-a-cyber-world-war/ [https://perma.cc/XKH2-UEVV] (quoting Smith's remarks to the November 2018 Web Summit conference in Lisbon).

[2] Lorenzo Franceschi-Bicchierai, *Ex-NSA Director Says Companies Should Never Hack Back Because They Could Start Wars*, VICE (Nov. 6, 2017), https://motherboard.vice.com/en_us/article/a37njb/keith-alexander-nsa-hack-back [https://perma.cc/3JZJ-FPA9] (quoting Alexander's address to the CyberConnect 2017 conference in New York City).

[3] The Council on Foreign Relations maintains a database of incidents publicly known (or publicly believed) to be state-sponsored since 2005. *See Cyber Operations Tracker*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/interactive/cyber-operations [https://perma.cc/CC5C-X9P8]. For another helpful database, see generally Ryan Maness, *The Dyadic Cyber Incident and Dispute Data, Version 1.5*, https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset [https://perma.cc/EY8E-XW5P].

[4] *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'l Sec. Tech. & L., Aegis Series Paper No. 1806, 2018), https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf [https://perma.cc/L8S9-X2AY].

sector.[5] To summarize the state of affairs in late-2019: (1) attackers in cyberspace have an undisputed advantage over defenders; [6] (2) inter-state cyber conflict outside an ongoing armed conflict has, to date, largely stayed below the use of force and armed attack thresholds in the United Nations Charter;[7] (3) few states have responded to malign cyber operations against their private sector with real-world lethal force, although some appear to have considered or responded with cyber countermeasures;[8] and (4) although the United States and allied governments are now said to be pursuing, at the nation-state level, policies of "active defense" and "defend forward" postures in cyberspace, it is hard in an unclassified setting to know how, how much, and how fast.[9]

---

[5] *See generally* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103 (2014). I return to this point and to this article in Section III, *infra*.

[6] "Cyber" is a notoriously unclear term. Here it simply means "pertaining to the internet." Wherever possible, this Article avoids even more notoriously unclear terms like "cyberattack" and "cyberwar."

[7] U.N. Charter arts. 2(4) & 51. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt, ed., 2nd ed. 2017) [hereinafter TALLINN 2.0] ("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 Distributed Denial of Service (DDoS) attack was an armed attack triggering NATO Article 5. *See also* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://www.wired.com/2007/08/ff-estonia/ [https://perma.cc/N2SZ-SJTZ].

[8] 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). Of note, though not this Article's focus, several states have either asserted or employed the right to respond to cyberattacks within an ongoing armed conflict with lethal force. @IDF, Twitter (May 5, 2019, 08:55 AM), https://twitter.com/IDF/status/1125066395010699264 [https://perma.cc/RA5W-R8TF] (Tweet announcing the Israel Defense Forces strike of May 5, 2019). *But see* Maness, *supra* note 3 (cautioning that, contrary to popular perception, relatively few state conflicts involve a (known) cyber component (yet)).

[9] *See*, *e.g.*, OFFICE OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/5C9H-JU4U]) (announcing the United States "defense forward" posture); CABINET OFFICE, NATIONAL CYBER SECURITY STRATEGY 2016 TO 2021, (Sept. 11, 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [https://perma.cc/3967-GFHM]) (announcing the United Kingdom's offensive posture); Nele Achten, *Germany's Position on International Law in Cyberspace*, LAWFARE (Oct. 2, 2018), https://www.lawfareblog.com/germanys-position-international-law-cyberspace [https://perma.cc/S2DY-9Z98]) (describing Germany's new conception of international law in cyberspace); Robin Emmott, *NATO Mulls "Offensive Defence" With Cyber Warfare Rules*, REUTERS (Nov. 30, 2017), https://uk.reuters.com/article/uk-nato-cyber/nato-mulls-offensive-defence-with-cyber-warfare-rules-idUKKBN1DU1GV [https://perma.cc/6T5W-V6NR]) (announcing NATO's new offensive posture); Arthur P. B. Laudrain, *France's New Offensive Cyber Doctrine*, LAWFARE (Feb. 26, 2019), https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine [https://perma.cc/YD8N-AQUT]) (describing France's new offensive cyber doctrine).

Meanwhile, the private sector feels under attack and unprotected. In response, one increasingly mainstream national security argument calls for amending U.S. law to permit private sector actors—some of the world's most technologically savvy transnational corporations and non-governmental organizations—to employ so-called "active defense" measures.[10]

The best summary of the mainstream understanding of active defense is a widely cited 2016 report put out by George Washington University's Center for Cyber and Homeland Security (CCHS) Active Defense Task Force.[11] The 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

[10] 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 in which 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 (July 26, 2012), https://www.securityweek.com/black-hat-survey-more-13-have-engaged-retaliatory-hacking [https://perma.cc/K9RM-FL4Q]. Additionally, a poll of 500 attendees at the 2019 RSA Conference 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 (Mar. 19, 2019), https://www.venafi.com/blog/cyber-war-grows-it-time-strike-back [https://perma.cc/5DL7-N7YN]; Without access to the underlying data, it is hard to assess the accuracy of such informal polls; here, I cite them solely for their part in the ongoing cyberwar narrative. For further quotes by senior government and non-governmental officials supporting such measures, see generally Joseph Cox, *Revenge Hacking is Hitting the Big Time*, DAILY BEAST (Sept. 19, 2017), https://www.thedailybeast.com/inside-the-shadowy-world-of-revenge-hackers [https://perma.cc/ZA3K-LUAK]; Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back [https://perma.cc/N387-UJV5].

[11] The Task Force was 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. Although the Task Force included some members long known for supporting an aggressive private sector role in cyberspace (e.g., Stewart Baker), it also 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, an active defense skeptic, served as consultant. DENNIS BLAIR ET AL., INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS (2016), https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf [https://perma.cc/WZR3-3NG3] [hereinafter CCHS Report]. For the skeptic's perspective, 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); Kerr, Volokh & Baker, *infra* note 15 (Kerr's portion of the debate held on the Volokh Conspiracy blog); *see also* Bruce Schneier, *Hacking Back*, SCHNEIER ON SECURITY (Feb. 13, 2017), https://www.schneier.com/blog/archives/2017/02/hacking_back.html [https://perma.cc/ZJG8-6H3X] ("I've never been a fan of hacking back . . . But the [CCHS Report] makes a lot of good points.").

> 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.[12]

On the *policy*, proponents assert that active defense measures could complement government defenses by slowing, identifying, or deterring offenders in cyberspace, providing evidence for use in civil cases, or supporting a government response,[13] while skeptics argue that careless or incompetent private sector actors in cyberspace may create more problems than they could solve, either by recklessly or negligently harming adversary (or intermediary) computers or by inviting counterretaliation.[14] *Legally*, however, active defense measures likely cannot be employed without running afoul of U.S. laws like the Computer Fraud and Abuse Act.[15]

The debate takes many forms. Some argue for aggressive offense by both private and public sectors;[16] others for a more measured set of private sector active defenses;[17] for abandonment of the active defense model in favor of other more

---

[12] CCHS Report, *supra* note 11, at xi.

[13] The bulk of the CCHS report is dedicated to outlining a framework that the authors believe would allow for the benefits without the drawbacks, one that "confirms government oversight, ensures that privacy and civil liberties are not infringed, and mitigates technical risks." CCHS Report, *supra* note 11, at v.

[14] Some lawyers and technologists have criticized active defense proponents as representing a radical position technically indistinguishable from aggressive hacking back. *See, e.g.*, Josephine Wolff, *When Companies Get Hacked, Should They be Allowed to Hack Back?*, THE ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ [https://perma.cc/HRL2-AW7M].

[15] For the key U.S. legal debates, see Orin Kerr, Eugene Volokh & Stewart Baker, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ [https://perma.cc/G98R-8HSK]. For an excellent history of policy, legal, and technical considerations in the private sector active defense discussion (and for a history of the *idea* of active defense more broadly), see, e.g., Sean Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12 (2014); Patrick Lin, *Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies* (Sept. 26, 2016), http://ethics.calpoly.edu/hackingback.pdf [https://perma.cc/K57P-4PRV]; For a collection of relevant articles dating back to the 1990s, see also Dave Dittrich's "active defense" reading list, https://web.archive.org/web/20161218084352/https://staff.washington.edu/dittrich/home/activeresponse.html [https://perma.cc/X88P-6HE5].

[16] *See, e.g.*, Kerr, Volokh & Baker, *The Hackback Debate*, *supra* note 15 (Baker comments); Stewart Baker, *Four principles to guide the US response to cyberattacks*, FIFTH DOMAIN (Feb. 7, 2019), https://www.fifthdomain.com/thought-leadership/2019/02/07/four-principles-to-guide-the-us-response-to-cyberattacks/ [https://perma.cc/82V2-S6F8].

[17] *See, e.g.*, CCHS Report, *supra* note 11.

productive models for acting on intelligence sharing;[18] for careful vetting of companies authorized to take certain active defense measures under the supervision of the U.S. government;[19] for caution given that the more oversight the government exercises over the private sector, the more likely state responsibility doctrine is to apply;[20] for a polycentric model;[21] and so on.

This Article does not try to resolve or take sides in those policy or legal arguments. Instead, it addresses just one striking aspect of the U.S. debate over active defense measures—how little other countries' laws enter the discussion.

B. *Research Problem*

To the extent that other countries' laws enter the discussion, proponents of active defense often assert, without citation, that other countries' laws are less stringent or somehow more permissive than the United States' laws,[22] while critics and skeptics suggest, again without citation, that all active defense measures are similarly unlawful—or similarly not clearly lawful—in all countries.[23]

These vague references confuse rather than advance the conversation. Other countries' domestic laws are important constraints on U.S. private sector behavior. If policymakers and private sector actors want to pursue active defense, there needs to be a better sense of what those foreign laws say—whether good, bad, or

---

[18] *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://www-cdn.law.stanford.edu/wp-content/uploads/2018/08/SLPR_Cook.pdf [https://perma.cc/9Q7W-SLR7].

[19] *See, e.g.*, Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up* 15–16 (Hoover Working Group on Nat'l Sec. Tech. & Law, Aegis Series Paper No. 1606, 2016), https://drive.google.com/file/d/0B_PclSuEzVCVYUo1bE5fUjFEMHM/view [https://perma.cc/8VKT-MRY8].

[20] *See, e.g.*, Kristen Eichensher, *Would the United States Be Responsible for Private Hacking?*, JUST SECURITY (Oct. 17, 2017), https://www.justsecurity.org/46013/united-states-responsible-private-hacking/ [https://perma.cc/HL5U-P9R7].

[21] *See, e.g.*, Craig, Shackelford & Hiller, *infra* note 24; Shackelford, Russell & Kuehn *infra* note 24.

[22] *See, e.g.*, Wyatt Hoffman, *The Future of Cyber Defense*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 17, 2018), https://carnegieendowment.org/2018/07/17/future-of-cyber-defense-pub-76892 [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 does not name specific permissive environments. For starting places to identify that transnational market, see generally, SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014); Craig, Shackelford & Hiller, *infra* note 24.

[23] In his 2014 article, Paul Rosenzweig cited Germany's "Hacker paragraph" as one known example of another country's relevant domestic law. Rosenzweig, *supra* note 5, at 114. Since Rosenzweig published in 2014, many articles have duly recited the German law, but few articles have looked for other examples, except as mentioned, *infra* note 24.

indifferent. This is an underdeveloped area of research.[24] There are few answers to straightforward descriptive questions, such as:

- What other countries have relevant laws?
- Are there foreign equivalents to the U.S. Computer Fraud and Abuse Act, the U.S. Wiretap Act, and the general U.S. prohibition on pen registers/trap and trace devices?
- Are any foreign equivalents more or less restrictive than the U.S. laws?

This Article is the first sizable study to answer some of those basic comparative questions. It collects in one place a handful of other countries' laws that might limit the private sector's ability to employ active defense measures, then compares them with each other and with our general understanding of relevant U.S. laws. Interestingly, mapping out the terrain in this way illustrates how domestic laws in many countries have converged to cover much of the same substantive ground.[25]

### C. *Roadmap*

Section II describes how four common examples of private sector active defense measures may implicate different types of laws, using U.S. law as an example. Section III comments on (the few) international laws and norms in cyberspace as they exist today. Section IV identifies and compares domestic laws from a number of countries, shows how many of these laws compare to the U.S. laws, and considers the differences between U.S. and other domestic laws. Section V draws some very basic conclusions and asks what this means for the future of the U.S. discussion around private sector active defense.

---

[24] I am aware of only a few examples of relevant academic research. *See* Rosenzweig, *supra* note 5; CCHS Report, *supra* note 11, at Appendix III (including a few paragraphs on active defense *climates* 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); 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 United States, Germany, and China).

[25] 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. *Cybercrime Repository*, UNITED NATIONS OFFICE ON DRUGS AND CRIME, https://sherloc.unodc.org/cld/v3/cybrepo/. For the study itself, see *Comprehensive Study on Cybercrime*, UNITED NATIONS OFFICE ON DRUGS AND CRIME (Feb. 2013), https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf [https://perma.cc/CB8V-CYEF]. As some laws hosted on the Cybercrime Repository 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. I provide citations to the most recent English text or translation publicly available in 2019 in the Appendix, *infra*.

## II. What is Private Sector Active Defense?

### A. *Basic Concepts*

This Article will examine four of the most commonly discussed active defense options.[26] A private sector active defender can create false files that lure attackers to locations where they may be more easily monitored (i.e., honeypots) or can block or redirect all unknown incoming internet traffic to a separate place for closer monitoring (i.e., sinkholes). If the defender fears that an attacker will steal data, the defender might implant code in their files that sends alerts back to the file owner if an attacker opens the file (i.e., beacons). If data is successfully stolen, the defender might want to follow the attacker's trail through the internet, looking for clues along the way (i.e., traceback techniques).

The technical side of active defense boils down to simple ideas like these, but each may be legally problematic. Before turning to other countries, it is important to examine how U.S. law applies to these four ideas.[27] This Article explains in brief and non-technical terms how each measure works and how each measure may implicate different types of laws.[28] As is so often the case, the constraints here are about legal uncertainty, not the certainty of prosecution.[29]

### B. *Four Examples*

#### 1. Honeypots

Honeypots are fake files, file structures, and servers that look real but are carefully segmented from a defender's real network. Ideally, they are designed to attract and isolate intruders, so they can be monitored without risk to the real network.[30] 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.[31]

---

[26] *See* CCHS Report, *supra* note 11; *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://www.heritage.org/sites/default/files/2017-05/BG3188.pdf [https://perma.cc/E22C-LWEB].

[27] The CCHS report, *supra* note 11, provides a fuller spectrum of examples; this Article focuses on just four.

[28] For more extensive technical explanation of each of these measures than I provide in this more abstracted summary, see Harrington, *supra* note 15.

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

[30] *See* CCHS Report, *supra* note 11, at 11.

[31] For a lay summary of different types of honeypots, see Greg Martin, *How to Use "Honeypots" to Overcome Cybersecurity Shortcomings*, POWER MAG. (Sept. 1, 2014), https://www.powermag.com/how-to-use-honeypots-to-overcome-cybersecurity-shortcomings/ [https://perma.cc/23M5-LV75].

Honeypots are problematic in jurisdictions that prohibit private sector actors from recording metadata absent a court order. In the United States, the legal question is unsettled. The CCHS Report concludes that honeypots set without government oversight may run afoul of the U.S. general prohibition on trap and trace devices.[32] A number of U.S. commentators have made similar comments,[33] with some arguing that current confusion could be resolved by simple (but not forthcoming) interpretive guidance from the U.S. Department of Justice (DOJ).[34] Even those who argue for the minority view—that honeypots don't violate the 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.[35] As a practical matter, honeypots are widely advertised and employed as cybersecurity measures,[36] despite public cautions from the DOJ that the law is "untested."[37]

2. Sinkholes

---

[32] CCHS Report, *supra* note 11, at 42. The prohibition on pen register and trap and trace (PRTT) devices is found in 18 U.S.C. § 3121 (2018). Originally drafted for the telephone age, the PRTT prohibition has been read to encompass Internet communications. A pen register device records outgoing metadata from network devices; a trap and trace device records incoming metadata. CCHS Report, *supra* note 11, at 42.

[33] *See, e.g.*, Cook, *supra* note 18, at 212; *see also* Rosenzweig, *supra* note 5.

[34] *See* Gregory Falco & Herb Lin, *Active Cyber Defense and Interpreting the Computer Fraud and Abuse Act*, LAWFARE (Dec. 21, 2018), https://www.lawfareblog.com/active-cyber-defense-and-interpreting-computer-fraud-and-abuse-act [https://perma.cc/73J8-46XX] (considering a hypothetical, Falco and Lin argue that it would be a relatively conservative expansion of current U.S. law to re-interpret 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).

[35] *See The Ethics of Hacking Back: Cybersecurity and Active Network Defense*, CARNEGIE COUNCIL (Sept. 18, 2013), https://www.carnegiecouncil.org/studio/multimedia/20130918-the-ethics-of-hacking-back-cybersecurity-and-active-network-defense [https://perma.cc/R9HL-4LDW] (comments of Robert Clark, at the panel discussion: "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 that, for U.S. lawyers at least, professional responsibility concerns arise when private sector attorneys are involved in deceptive actions. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 8.4(c) (AM. BAR ASS'N 1983); Harrington, *supra* note 15, at 15.

[36] *See, e.g.*, Michael Kassner, *DarkMatter: Curing the Internet of Digital Threats*, TECHREPUBLIC (Aug. 1, 2014), https://www.techrepublic.com/article/darkmatter-curing-the-internet-of-digital-threats/ [https://perma.cc/WR8U-6NXV] (describing U.S.-based Norse Corporation's global network of eight million honeypots tracking the spread of malware in real time).

[37] William Jackson, *Dangers in Luring Hackers with Honey*, GCN (Aug. 2, 2002), https://gcn.com/articles/2002/08/02/dangers-in-luring-hackers-with-honey.aspx [https://perma.cc/5KEU-VBM4] (quoting Richard Salgado, then of the DOJ Computer Crime and Intellectual Property Section (CCIPS)). The law is still unclear and untested. *See also ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. On the Judiciary*, 111th Cong. 17–18 (2010) (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.) (explaining that the law is full of "complex and baffling rules" in the face of modern challenges).

The internet operates, at a very basic level, by (1) dividing data up into small packets; (2) labelling each packet with a numerical Internet Protocol (IP) address marking its destination (along with its origin and other metadata); and (3) sending those packets up and down a hierarchical series of routers until all the packets reach their collective destination and can be reassembled into a readable file or executable program. But IP addresses are strings of numbers, not words (e.g., 2606:2800:220:1:248:1893:25c8:1946). To find the IP address that is the digital equivalent of *www.example.com*, the computer uses the Domain Name System (DNS).[38] It is helpful to think of the DNS as a phonebook, translating between names and numbers.

Sinkholes redirect internet traffic by intervening in the translation of a domain name to the corresponding IP and replacing it with the sinkhole IP. That is, they provide a false number/address in the phonebook, which typically requires coordination with the relevant Internet Service Provider (ISP) or DNS registrar. 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, so-called "botnet takedowns".[39]

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."[40] 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.[41] 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.[42] Others have noted that, as a practical matter, even if sinkholing without a court order were clearly lawful, the ISP or DNS registrar may lack any incentive to help.[43]

Notably, the 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

---

[38] For a basic technical overview with helpful diagrams, see, e.g., Rus Shuler, *How Does the Internet Work?* (2002), https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm [https://perma.cc/S82Z-MRJL].

[39] *See What is a DDoS Botnet*, CLOUDFARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet [https://perma.cc/R7P2-J9JA]; Starting in 2011, the DOJ has used sinkholes to take down botnets. *See, e.g.*, Brian Krebs, *U.S. Government Takes Down Coreflood Botnet*, KREBS ON SECURITY (Apr. 14, 2011), https://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet [https://perma.cc/BM2C-3FXA].

[40] CCHS Report, *supra* note 11, at 42; *see also* 18 U.S.C. § 3121 (2018).

[41] For the implications of private sector actors working more closely with law enforcement, *see, e.g.*, Eichensehr, *supra* note 20.

[42] CCHS Report, *supra* note 11, at 42; *see also* 18 U.S.C. § 2510 (2018) *et seq.*

[43] *See* Harrington, *supra* note 15, at 17–18.

> 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."[44]

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 against 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.[45]

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."[46] Alternatively, 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"[47]—to "phone home" with details about the route the file has taken or where it currently may be.

Although beacons may seem harmless and sensible, in that they simply serve as alarms for stolen information, by design they may involve unauthorized viewing or obtaining of data on another's computer and potentially also execution of a program on another's computer.[48] In the United States, this is generally seen

---

[44] U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES App. D at 182 (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/5NVA-YHW8] [hereinafter DOJ Manual].

[45] *Id*. at 180; *see also infra* note 61.

[46] Shaun Waterman, *Clarity Needed on "Active Defense" by Cyber-Victims: Report*, CYBERSCOOP (Oct. 31, 2016), https://www.cyberscoop.com/gwu-cchs-hacking-back-active-defense-by-cyber-victims/ [https://perma.cc/3JW9-82LW].

[47] Paul Rosenzweig, Steven P. Bucci & David Inserra, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, HERITAGE FOUNDATION (May 5, 2017), https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf [https://perma.cc/VNG2-9QGF].

[48] *See also* blog comment by Dave Dittrich (Feb. 14, 2017 at 6:16 pm) on Schneier, *supra* note 11 (cautioning that beacons neither give "as accurate an attribution as an unsophisticated technical

as violating the 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,[49] [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."[50]

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.[51] 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 is, at best, untested.[52] To resolve some of the uncertainty surrounding beacons, the Active Cyber Defense Certainty Act was

analysis may suggest" and that "someone who doesn't know what they are doing will shoot back at the wrong party").

[49] 18 U.S.C. § 1030(a)(2) (2018). "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) (2018). The 7th and 8th Circuit Courts of Appeals 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. *See* 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, *supra* note 44, at 4–5 (summarizing legislative history and noting that even computers not connected to the internet may meet this definition).

[50] 18 U.S.C. § 1030(a)(5) (2018).

[51] *See generally* Kerr et al., *supra* note 15.

[52] *See, e.g.*, CCHS Report, *supra* note 11, at 41 (failing to reach a final conclusion on how much legal risk beacon use would incur); Cook, *supra* note 18, at 212.

introduced in Congress in 2017 to expressly permit phone home beacons, but never made it out of committee.[53] As of mid-2019, it is once again being introduced.[54]

4. Traceback Analysis

Technologically adept companies can sometimes trace a thief or attacker's trail through the internet using a variety of techniques.[55] Note that tracing data through the internet "means passing through every server the attacker has compromised."[56] 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 United States, this generally means that the tracker is violating the CFAA.[57]

The most well-known example of a U.S. company "following the trail" is the case of Google's response to "Operation Aurora" in 2009–10. After Google became aware of a "highly sophisticated and targeted attack on [its] corporate

---

[53] H.R. 4036, 115th Cong. (2017). As drafted in 2017, § 3 would have inserted 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 (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html [https://perma.cc/GZS6-CUCX] (criticizing the draft Act generally, but calling the beaconing provisions reasonable).

[54] *See* Robert Chesney, *Hackback is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019), https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act [https://perma.cc/72BJ-8N7Q].

[55] *See generally* Shane Harris, *The Mercenaries*, SLATE (Nov. 12, 2014), https://slate.com/technology/2014/11/how-corporations-are-adopting-cyber-defense-and-around-legal-barriers-the-emergence-of-cybersecurity-mercenaries-is-changing-the-future-of-cyberwar.html [https://perma.cc/Z8WN-WGA8] (excerpting from HARRIS, *supra* note 22).

[56] 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 [https://perma.cc/AZK4-CXMY] (providing an overview of the technology and terminology of "hack back" as it was in 2002 and illustrating how little the basic arguments have changed, even as the internet has expanded).

[57] *See* CCHS Report, *supra* note 11, at 14–15.

infrastructure," the company traced the attack back to a server in Taiwan, where Google found information that led it to accuse China.[58] Neither Google nor the U.S. government have confirmed or denied publicly whether Google had permission to enter the Taiwanese server, 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."[59] 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.[60] The CCHS Report notes that, "[t]o 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."[61]

In another example of a more offensive traceback operation, in 2015, the Israeli security firm Check Point accessed the phishing and command-and-control servers of the Rocket Kitten group (allegedly linked to Iran), thereby identifying both victims and a number of alleged perpetrators.[62] Its public report of the investigation demonstrates in an unclassified setting what investigative measures may be technically possible.[63] 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.[64] The episode illustrates the fine legal line that those conducting private intelligence analysis walk and sometimes may cross.

C. *Summary*

---

[58] David Drummond, *A New Approach to China*, GOOGLE OFFICIAL BLOG (Jan. 12, 2010), https://googleblog.blogspot.com/2010/01/new-approach-to-china.html [https://perma.cc/2T8Y-2QPL].

[59] HARRIS, *supra* note 22, at 172.

[60] *See* CCHS Report, *supra* note 11, at 14–15, 40. I am unaware of any U.S. analysis of the episode that references 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).

[61] CCHS Report, *supra* note 11, at 14 (citing language from a DOJ Computer Crime & Intellectual Property Section (CCIPS) white paper, which updated, without changing the substance, the 2010 language cited *supra* note 44; *see* U.S. DEP'T OF JUST., BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf [https://perma.cc/QG52-MN9P]).

[62] *See* CHECK POINT SOFTWARE TECHNOLOGIES, ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES (2015), https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf [https://perma.cc/RF6C-9NQT].

[63] *Id.*

[64] *See* Eduard Kovacs, *Hacking Back: Industry Reactions to Offensive Security Research*, SECURITY WEEK (Nov. 13, 2015), https://www.securityweek.com/hacking-back-industry-reactions-offensive-security-research [https://perma.cc/28RR-BU37] (quoting reactions of Kaspersky Lab, Raytheon, RSA, etc.).

Active defense boils down to ideas like these, all of which can be legally problematic in the United States for the reasons explained above. Again, keep in mind that the constraints here are about legal *uncertainty*, not the certainty of prosecution. 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 analysis may well 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?

## III. A Brief Note on International Law

To state something very basic but not necessarily intuitive: no formal source of international law directly bars private sector actors, acting on their own, from using the active defense measures described above.[65] The first international treaty addressing crimes committed on the internet, the Budapest Convention on Cybercrime,[66] calls on its signatories to criminalize a number of actions dealing with access to computer systems or interception of non-public computer data.[67] But the Budapest Convention is not self-executing, has been ratified by only sixty-two

[65] *See, e.g.*, Rosenzweig, *supra* note 5, at 104 (generally concluding 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* Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, STRATEGIC STUD. Q. 126 (2012), https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Brown-Poellet.pdf [https://perma.cc/765N-CGY3]; CCHS Report, *supra* note 11.

[66] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185 (entered into force Jul. 1, 2004), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [https://perma.cc/GDU2-QX6L] (hereinafter "Budapest Convention").

[67] 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.

mostly European states parties (many with reservations),[68] and is thought only to hint at an emerging set of norms.[69]

Paul Rosenzweig has argued that the Budapest Convention's repeated use of the term *without right* 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.[70] This widely cited argument, however convincing, is so far merely academic; it has not yet and may never be raised before any formal body. 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."[71] 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.[72] Outside of the Budapest framework and the unofficial Tallinn attempts to codify the law as it is believed to exist today, other international soft law projects have made headlines but, as yet, lack tangible results.[73]

---

[68] CHART OF SIGNATURES AND RATIFICATIONS OF TREATY 185 (Jan. 1, 2019), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Wyx2E23q [https://perma.cc/DW2J-NWU9].

[69] U.S. ratification prompted criticism from all sides, but now those concerns seem to have been overblown. For a contemporaneous news article, see Nate Anderson, *"World's Worst Internet Law" Ratified by Senate*, ARS TECHNICA (Aug. 4, 2006), https://arstechnica.com/uncategorized/2006/08/7421/ [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 INSTITUTION (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf [https://perma.cc/S4NW-NU9H] (telling a cautionary tale about what the Budapest Cybercrime Convention suggests for future cyber-treaties).

[70] *See* Rosenzweig, *supra* note 5; *see also* Council of Europe, *Explanatory Report to the Convention on Cybercrime* (Nov. 23, 2001), https://rm.coe.int/16800cce5b [https://perma.cc/3VRZ-ECR9]; Sharon Cardash & Taylor Brooks, *Mounting an Active Defense Against Cyber Threats*, INTERNATIONAL PEACE INSTITUTE GLOBAL OBSERVATORY (Nov. 10, 2016), https://theglobalobservatory.org/2016/11/cybercrime-active-defense-mirai-botnet/ [https://perma.cc/2ZR7-JV7V]; 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://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense [https://perma.cc/RSY9-S6B8].

[71] TALLINN 2.0, *supra* note 7, Rule 4.

[72] TALLINN 2.0, *supra* note 7, Rule 4; *c.f.* Rules 15 and 17.

[73] The 2016–17 United Nations Group of Governmental Experts, convened to consider applicable norms, failed to come to consensus. *See* Adam Segal, *The Development of Cyber Norms at the*

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.[74] States have yet to adopt these theories. For now, it seems the final word is 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."[75]

## IV. A Survey of Domestic Laws

### A. *Countries to Examine*

As mentioned in Section I, one claim sometimes made in the conversations on active defense measures is that companies that operate in more permissive legal jurisdictions are driving this activity.[76] But, if that is true, which of these unnamed jurisdictions are "permissive" and how might they be identified?

---

*United Nations Ends in Deadlock. Now What?*, COUNCIL ON FOREIGN RELATIONS BLOG (June 29, 2017), https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what [https://perma.cc/T8JQ-WTW4]; Arun Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (July 4, 2017), https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well [https://perma.cc/2WB6-JBDS]. The Paris Call 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," and has the 370 signatories, including all 28 members of the European Union, 27 of the 29 NATO members, and private sector companies including Microsoft, Google, Facebook, Intel, Citigroup, and Visa, among others. *See Paris Call for Trust and Security in Cyberspace* (Nov. 12, 2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf [https://perma.cc/C6QV-SXZ8]. Microsoft's call for a Digital Geneva Convention asks states to pledge not to attack private corporations. Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT BLOG (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [https://perma.cc/3M5H-4MPK]; Brad Smith, *34 Companies Stand Up for Cybersecurity With a Tech Accord*, MICROSOFT BLOG (Apr. 17, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/ [https://perma.cc/XC27-6ET2] (showing related Cybersecurity Tech Accord, signed by thirty-four companies, promising not to help governments launch cyberattacks against innocent citizens and enterprises).

[74] *See, e.g.*, Rosenzweig, *supra* note 5, at 110–13; *see also* Wyatt Hoffman & Ariel Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 14, 2017), https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf [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 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 generally* Eichensher, *supra* note 20.

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

[76] *See* Hoffman, *supra* note 22.

This Article reviews a manageable, yet diverse, dataset of countries' domestic laws, selected based on the merger of a number of rankings of states that lead across a broad set of cybersecurity measures,[77] states that are the home jurisdictions for the world's largest companies,[78] states that are the home jurisdictions for the world's cybersecurity companies,[79] states that are commonly said to be the world's most powerful state cyber powers,[80] and states that comprise the world's most powerful military powers generally.[81]

Twenty states appear repeatedly on those lists. This Article surveys this limited group: Australia, Canada, China, Estonia, France, Germany, Iran, Israel, Japan, the Netherlands, Oman, Russia, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan,[82] United Kingdom, and United States. While understanding that any methodology for selection inevitably leaves out important players, this diverse group includes large and small states, U.S. allies and non-allies, various forms of democracies and non-democracies, civil and common-law jurisdictions, and twelve states party to the Budapest Convention and eight non-parties.[83]

B. *What Questions to Ask?*

---

[77] *See Global Cybersecurity Index (GCI) 2017*, INT'L TELECOMM. UNION (July 19, 2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf [https://perma.cc/JH62-DPAR]; *c.f.*, Bhaskar Chakravorti, Ajay Bhalla & Ravi Shankar Chaturvedi, *60 Countries' Digital Competitiveness, Indexed*, HARV. BUS. REV. (July 12, 2017), https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed, [https://perma.cc/CA66-5B4M].

[78] *See Global Top 100 Companies by Market Capitalization*, PRICEWATERHOUSECOOPERS (updated Mar. 31, 2018), https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2018-report.pdf [https://perma.cc/X8BK-BPZS].

[79] *See* Steve Morgan, *Cybersecurity 500 by the Numbers: Breakdown by Region*, CYBERCRIME MAG. (May 21, 2018), https://cybersecurityventures.com/cybersecurity-500-by-the-numbers-breakdown-by-region/ [https://perma.cc/33QQ-SRVJ?type=image]; *see also Cybersecurity 500 2018: The Official List*, PR NEWSWIRE (May 15, 2018), https://www.prnewswire.com/news-releases/cybersecurity-500-2018-the-official-list-300648938.html [https://perma.cc/KM86-XFFG] (explaining the methodology with which Cybersecurity Ventures made their selection of the top 500).

[80] *See, e.g.*, Shannon Vavra, *The World's Top Cyber Powers*, AXIOS (Aug. 13, 2017), https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html [https://perma.cc/7SVG-NAGA] (identifying China, Iran, Israel, North Korea, Russia, the United States, and the United Kingdom).

[81] *See 2019 Military Strength Ranking*, GLOBAL FIREPOWER, https://www.globalfirepower.com/countries-listing.asp [https://perma.cc/8CLY-ENUZ].

[82] This Article takes no position on the legal status of Taiwan other than noting it has a set of relevant laws and is the home jurisdiction for some of the world's largest companies and cybersecurity companies.

[83] *See supra* note 68. No methodology is unassailable and this Article does not assert that this list of twenty is the best or only such list, merely that this mashup of both objective and subjective rankings provides enough diversity to support the very basic points made in Section IV. If expanded, the next five countries in the survey would be Egypt, Malaysia, Mauritius, Ireland, and Brazil.

As seen in Section II, *supra*, the U.S. conversation about the legality of active defense measures generally orbits around 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;[84] the Wiretap Act, which prohibits intercepting communications without a court order (or equivalent defined by law);[85] and the prohibition on pen register and trap and trace devices—devices or programs that collect, respectively, outgoing and incoming metadata.[86]

C. *What Do States Formally and Clearly Prohibit?*

The first question, then, is a basic one: which other states, if any, have laws that might similarly restrict private sector activity? Table 1 simply lays out which states have laws governing the following five types of activity:

> (1) laws that prohibit access without right to a computer system—which presumably constrains the use of beacons and certain traceback analysis methods;
> (2) laws that prohibit 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;
> (3) laws that prohibit interception without right of non-public transmissions of computer data—which presumably constrains the use of some sinkholes and honeypots;
> (4) laws that prohibit 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;
> (5) laws that prohibit the production, sale, procurement, import, or distribution or any device, program, or data designed or adapted primarily for the purpose of committing the previous offenses. Although not directly related to the active defense measures debate, these last types of provisions have implications for public-private

[84] 18 U.S.C. § 1030 (2018) *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]).
[85] 18 U.S.C. § 2510 (2018) *et seq*.
[86] 18 U.S.C. § 3121 (2018).

> information sharing and security testing, so I've included them here as a relevant part of the map; and
> 6) finally, which, if any, states have laws that would explicitly permit or except active defense measures from the laws in the five prior columns.

A few administrative notes: The Appendix to this Article provides Bluebook citations with permalinks to the most recent English text or translation publicly available in 2019. Because full citations are listed in the Appendix, cited laws in the tables do not have corresponding footnotes in each cell of the table (also, note that Estonian laws may include superscript characters, not to be confused with footnotes). Moreover, in the body of this Article and in tables, states are listed alphabetically by their common names. Formal names are used in the Appendix.

Table 1: Do states have laws formally and clearly prohibiting types of 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? *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** | | |
| **Japan** | Unauthorized Computer Access Law [UCAL][87] 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[88] | |
| **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 | |

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

[88] Japan recorded a reservation to the Budapest Convention, reserving the right not to apply Article 6, paragraph 1, except for: (a) the offences set forth in Article 168-2 or Article 168-3 of the Penal Code; and (b) the offences set forth in Article 4, 5, and 6 of the UCAL. *Supra* note 83, Japanese Reservation.

| 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[89] Art. 48(1); Infrastructure Protection Act[90] 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. 144$^{bis}$ | Criminal Code Art. 143 | Criminal Code Art. 144$^{bis}$ | Criminal Code Art. 143$^{bis}$ & 144$^{bis}$ | |
| **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.* |

[89] The full name is the "Act on Promotion of Information and Communications Network Utilization and Data Protection, etc."
[90] The full name is the "Act on the Protection of Information and Communications Infrastructure."

D. *Preliminary Comments*

Before going into more detail, this Article pauses to identify 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 codes, while others have a standalone computer code (i.e., Iran, Israel,[91] Japan, Oman, Singapore, and United Kingdom). Several place the general prohibition on intercepting communications in transit in their respective government surveillance codes (i.e., Israel, Taiwan, United Kingdom, and United States) 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 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.[92] Many of the Budapest states parties surveyed here issued reservations on substantive or jurisdictional points—or both.

For reference, China, Iran, Oman, Russia, Singapore, South Korea, Sweden, and Taiwan *are not* party to the Budapest Convention.[93] Australia, Canada, Estonia, France, Germany, Israel, Japan, the Netherlands, Spain, Switzerland, the United Kingdom, and the United States *are* parties.[94] Yet, the laws of Singapore, a non-party, have more in common with Canada's laws than Canada's laws have with German or Japanese laws. By the same token, 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

---

[91] 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). That article also includes some interesting comments on the United Kingdom's Computer Misuse Act.

[92] Budapest Convention, *supra* note 66.

[93] *See* CHART OF SIGNATURES, *supra* note 6883. Interestingly, Sweden signed but did not ratify the Convention.

[94] *See* CHART OF SIGNATURES, *supra* note 68.

Before discussing differences,[95] it is important to note that there are no obvious gaps, empty boxes, or obviously *permissive* jurisdictions in this initial survey. What are the implications 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.[96] 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 is either 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.

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 has contemplated.[97] If the United States were to pass something like H.R. 4036, the Active Cyber Defense Certainty Act, it would be an immediate outlier. Like the United States, Israel has draft active defense language in a bill under consideration but, like the United States, nothing is yet law.[98] However, no other countries appear to have comparable legislation under consideration.[99]

---

[95] In Sections IV.E through IV.J, *infra*, this Article delves into more subtle legal distinctions.

[96] Another facet of the now-foundational insight that "code is law." LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006), http://www.codev2.cc/ [https://perma.cc/4PWM-GY6H].

[97] *See* Craig, Shackelford & Hiller, *supra* note 24, at 739–45 (focusing on only one type of law (unauthorized access) in eight countries (the G8), but coming to a similar conclusion).

[98] *See* Haim Ravia & Dotan Hammer, *Israel: Cybersecurity 2020*, in 3 INTERNATIONAL COMPARATIVE LAW GUIDE 115, 117 (Nigel Parker & Alexandra Rendell et al. eds., 2019), https://www.law.co.il/media/knowledge-centers/cyb20_chapter_17_israel.pdf [https://perma.cc/3A73-JNR4] ("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."). 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 (June 20, 2018), https://www.law.co.il/en/news/2018/06/20/memorandum-israeli-cyber-law-published/ [https://perma.cc/N3YU-TYZF].

[99] Craig, Shackleford & Hiller, *supra* note 24, 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 2013–18 law, see Computer Misuse and Cybersecurity Act 1993, c. 50A, § 15A, https://sso.agc.gov.sg/Act/CMA1993/Historical/20130313?DocDate=20170511&ValidDate=20130313&ProvIds=P1III-#pr15A- [https://perma.cc/RBR6-WMY2]. For the current law, see Computer Misuse Act 1993, c. 50A, §§ 1–9, https://sso.agc.gov.sg/Act/CMA1993 [https://perma.cc/4WGF-9Y58]; Cybersecurity Act 2018, § 23, https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&ViewType=Pdf&_=20180904203749 [https://perma.cc/XKC6-3US9].

By contrast, some states have structures and procedures for government oversight of 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 explicitly reserve the right to employ active defense measures to the state (e.g., Estonia and the Netherlands). A number of states have guidelines for imposing criminal liability rules on corporations and groups.[100]

4. Extraterritorial Jurisdiction

Comparative jurisdiction deserves its own intense study.[101] The relevant U.S. laws were made explicitly extraterritorial in 2001.[102] This Article only notes that most of the states surveyed assert extraterritorial jurisdiction, in some form or another, over computer crimes. This is 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."[103]

A few countries have slightly more nuanced rules or phrasings. Iran asserts jurisdiction over any crimes where the data involved was in any way stored in or carried through Iranian telecommunications systems.[104] Interestingly, Japan asserts jurisdiction by reference to the Budapest Convention.[105] Singapore's extraterritorial jurisdiction language encompasses not only cases where the "computer, program or data was in Singapore at the material time" but also cases where "the offence

---

[100] *See infra* Section IV.J.

[101] For theories of how extraterritorial jurisdiction may be justified, see generally Harvard Research in International Law, *Jurisdiction with Respect to Crime*, 29 AM. J. INT'L L. SUPP. 435 (1935).

[102] *See* DOJ Manual, *supra* note 44, at 115–16.

[103] BROTTSBALKEN [BRB] [Penal Code] 2:4 (Swed.); *accord* 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. 12/11, 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).

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

[105] 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 [https://perma.cc/PKL6-AEQ3]. Because Japan is a Budapest Convention party, these nested provisions provide the requisite hook; *see also* Hiromi Hayashi, *Japan: Cybersecurity 2019*, INTERNATIONAL COMPARATIVE LAW GUIDE (Oct. 16, 2018), https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan [https://perma.cc/EN77-9RGR] (indicating that this is indeed how Japanese law asserts extraterritorial jurisdiction).

causes, or creates a significant risk of, serious harm in Singapore."[106] By contrast, Canada lacks statutory language on point for computer crimes, but employs the common law in appropriate circumstances to assert jurisdiction.[107]

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 2020 would forget to secure their data with basic security measures? 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.[108] 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.[109] The larger dataset was not secured until Bloomberg contacted Facebook for comment on April 3.[110]

---

[106] Computer Misuse Act 1993, c. 50A § 11(3) (Sing.) (defining serious harm 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* CCHS Report, *supra* note 11.

[107] Section 7 of their Criminal Code contains extraterritorial provisions for specified crimes, but that section does not include computer crimes. However, Canadian courts under the common law may extend territorial jurisdiction over offenses with a "real and substantial connection" to Canada (e.g., part of the offence or substantial effects in Canada). Canada recently explained as much when writing to the Office of Legal Affairs of the United Nations. *See* Permanent Mission of Canada to the United Nations, *Government of Canada Compilation of National Provisions on Criminal Accountability for UN Officials or Experts on Mission*, PRMNY-2886 (June 9, 2016), https://www.un.org/en/ga/sixth/71/criminal_accountability/questionnaire_canada_e.pdf [https://perma.cc/H2S2-RA5Q].

[108] *Losing Face: Two More Cases of Third-Party Facebook App Data Exposure*, UPGUARD (Apr. 3, 2019), https://www.upguard.com/breaches/facebook-user-data-leak [https://perma.cc/K6SE-PLPG].

[109] *Id.*

[110] *Id*.

The U.S. CFAA at least facially bans unauthorized access to *all* computer data.[111] Of the states surveyed here, that ban puts the U.S. in a group with Canada,[112] China,[113] France,[114] Israel,[115] Oman,[116] Russia,[117] Singapore,[118] South Korea,[119]

---

[111] 18 U.S.C. § 1030(a)(2); *see also* DOJ Manual, *supra* note 44, 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); *but see* Orin Kerr, *Scraping a Public Website Doesn't Violate the CFAA, Ninth Circuit (Mostly) Holds*, THE VOLOKH CONSPIRACY, (Sept. 9, 2019), https://reason.com/2019/09/09/scraping-a-public-website-doesnt-violate-the-cfaa-ninth-circuit-mostly-holds/ [https://perma.cc/X4T7-YMFY] (discussing a line of recent cases in the 9th Circuit that collectively define "unauthorized" in a more nuanced way).

[112] Canada Criminal Code, R.S.C. 1985, c C-46 § 342.1 ("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 . . . .").

[113] 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. 283–87 (China) ("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 . . . .").

[114] CODE PÉNAL [C. PÉN.] [Penal Code] art. 323-1 (Fr.) ("Fraudulently accessing or remaining within all or part of an automated data processing system is punished by . . . .").

[115] Computers Law 5755-1995, § 4, A.G. Pub., 2015 (Isr.) ("Whoever unlawfully penetrates computer material that is in a computer shall be liable . . . ."). The Israeli Supreme Court has read this section in the broadest possible sense, covering any access without clear permission or other affirmative legal authority. 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://www.law.co.il/en/news/2015/12/18/IL-high-court-defines-unauthorized-access-to-computer/ [https://perma.cc/8BS5-VFHP].

[116] Royal Decree No. 12/11, Issuing the Cyber Crime Law, art. 3 (Oman) ("Everyone who intentionally and illegally access [sic] 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.").

[117] UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 272 (Russ.) ("Illegal access to legally-protected computer information, if this deed has involved the . . . copying of computer information, - is punishable . . . ."); *see generally* Vasily Torkanovskiy, *Russia*: *Business Crime 2019*, INT'L COMP. L. GUIDE TO BUS. CRIME LAWS AND REGULATIONS (Dec. 9, 2018), https://iclg.com/practice-areas/business-crime-laws-and-regulations/russia [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").

[118] Computer Misuse Act 1993, c. 50A § 3 (Sing.) ("[A]ny 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.").

[119] Act on Promotion of Information and Communications Network Utilization and Data Protection, etc., Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, art. 48(1) (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do [https://perma.cc/U2GW-BVQZ] ("No one shall intrude on an information and communications network without a rightful authority for access or beyond a permitted authority for access.").

Sweden,[120] and the U.K.[121] By contrast, eight states criminalize access to data only if it is protected by a security measure (Australia,[122] Estonia,[123] Germany,[124] Iran,[125] Japan,[126] Netherlands,[127] Switzerland,[128] and Taiwan[129]) or if unrestricted data is accessed predicate to another offense (Australia[130]).

Those groupings are not 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). One longstanding argument in the U.S. legal academy is that the CFAA should be amended to "limit

---

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

[121] Computer Misuse Act 1990, c. 18, § 1 (Eng.) ("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 . . . .").

[122] *Criminal Code Act 1995* (Cth) ch 10 pt 6 s 478.1 (Austl.) ("A person is guilty of an offence if: (a) the person [intentionally] causes any [knowingly] unauthorised access to . . . *restricted data* . . . .") (emphasis added).

[123] KARISTUSSEADUSTIK [Penal Code] c. 13 § 217 (Est.) ("Illegal obtaining of access to computer systems *by elimination or avoidance of means of protection* is punishable . . . .") (emphasis added).

[124] STRAFGESETZBUCH [StGB] [Penal Code] § 202a (Ger.) ("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 . . . .") (emphasis added).

[125] MAJMUAHI QAVANINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1381 [2002], art. 726 (Iran) ("Every person who, without authority, gains access to data, or computer or telecommunication systems *which are protected under security measures* shall be punished . . . .") (emphasis added).

[126] 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) ("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*.") (emphasis added).

[127] Art. 138ab SR (Neth) ("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*.") (emphasis added).

[128] SCHWEIZERISCHES STRAFGESETZBUCH [StGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757, art. 143 (Switz.) ("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 . . . .") (emphasis added).

[129] 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 (Taiwan), https://law.moj.gov.tw/Eng/index.aspx ("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 . . . .") (emphasis added).

[130] *See Criminal Code Act 1995* (Cth) ch 10 pt 6 s 477.1 (Austl.) ("[Prohibits access 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, *High Tech Crime Brief: Hacking Offenses*, AUSTRALIAN INSTITUTE OF CRIMINOLOGY (Jan. 1, 2005) (describing the history of Australia's decision to set a higher bar for criminalizing access), https://aic.gov.au/publications/htcb/htcb005 [https://perma.cc/24XQ-GA5C].

the scope of unauthorized access statutes to circumvention of code-based restrictions on computer privileges," as is done in the latter group of eight countries.[131] This survey would seem to indicate that it is 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 and for any access to (unprotected but) private data generally.[132] 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.[133] The U.K. and Singapore make clear that the act "need not be 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."[134] Several states have thorough definitions for the key term *unauthorized*, while some, including the U.S., leave it undefined.[135]

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 views the offense; however, in the absence of reliable comparative data about actual prosecutions, it is the measure available.

---

[131] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003), https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-78-5-Kerr.pdf [https://perma.cc/R4C2-6MDQ]; *see also* CCHS Report, *supra* note 11, at 39 (expressing the additional views of Nuala O'Connor, writing separately to argue 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); *c.f.* Andrew Sellers, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221625 [https://perma.cc/AR4D-ARWH] (arguing that the courts have gone through three distinct eras in interpreting CFAA "authorization" in the context of web scraping).

[132] *Compare* CÓDIGO PENAL [C.P.] [Criminal 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 . . . .") *with* CÓDIGO PENAL [C.P.] [Criminal Code] art. 197 (Spain) (protecting data of a "personal or family nature" accessed "by any means").

[133] Royal Decree No. 12/11, Issuing the Cyber Crime Law, arts. 3–6 (Oman).

[134] Computer Misuse Act 1990, c. 18, § 1 (U.K.); *accord* Computer Misuse Act 1993, c. 50A, § 3 (Sing.).

[135] *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.).

Table 2: Maximum Penalties for Unauthorized Access[136]

| *State* | *Simple access (Months)* | *Access to restricted data (Months)* | *Access to government or critical infrastructure data (Months)* |
|---|---|---|---|
| Australia | N/A | 24 | 60 to life[137] |
| Canada | 120 | --[138] | -- |
| China | 36 | -- | 36 |
| Estonia | N/A | 36 | 60 |
| France | 24 | -- | 60 |
| Germany | N/A | 36 | -- |
| Iran | N/A | 91 days–12 months | -- |
| Israel | 36 | -- | -- |
| Japan | N/A | 36 | -- |
| Netherlands | N/A | 12–48 | -- |
| Oman | 1–6 | -- | 12–36 |
| Russia | 24 | -- | 24–60 |
| Singapore | 24 | -- | -- |
| South Korea | 60 | -- | 120 |
| Spain | 12–48 | -- | -- |
| Sweden | 24 | -- | -- |
| Switzerland | N/A | 60 | -- |
| Taiwan | N/A | 36 | 54 |
| United Kingdom | 24 | -- | -- |
| United States | 60[139] | -- | 120 |

[136] To avoid filling up the bottom of each page with endless citations, here and in successive pages, this Article generally footnotes only particularly interesting points. Other citations can be identified by referring to Table 1 and the Appendix.

[137] 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).

[138] 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.

[139] 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

The most striking takeaway from this rough 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 notional penalties in the one- to three-year range.

F. *Nuances in Modifying Data Laws*

Proponents of active defense measures often explicitly exclude or disavow aggressive *hack-backs*. However, laws that prohibit damage, deletion, deterioration, alteration, or suppression of computer data without right are still a necessary part of the discussion around active defense measures. Why? Because and *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.

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 modification of data as akin to traditional mischief or fraud.[140]

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."[141] 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

---

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 provides a helpful chart to keep track of the various factors. *See supra* note 44, at 3.

[140] *See, e.g.*, Arts. 350a & 350b SR (Neth.) (placing destruction or altering of computer data 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.) (placing "mischief in relation to computer data" as a subparagraph within the basic crime of mischief or destruction of property); In general, the Japanese law focuses on the harm that flows from access, rather than on the access itself. KEIHŌ [PEN. C.] 1907, arts. 161-2, 234-2, 246-2 & 259 (Japan) (framing the crime as one of harm to a business, property, right, or duty).

[141] *But see* Canada Criminal Code, R.S.C. 1985, c C-46 arts. 342.1 & 430 (Can.) (making most computer crimes punishable by up to ten years in prison, without gradations).

those circumstances "serious" is not defined within that law.[142] By contrast, Russia has one of the very few laws that defines "major damage" with a specific value: as exceeding one million rubles.[143]

The German law, to give another example, gives no firm criteria for distinguishing between the basic crime of deleting data, punishable by three years 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.[144] 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.[145]

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 data alteration 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 United States is again at the high end of the spectrum, along with Canada, China, South Korea, and the United Kingdom. However, every country has a substantial jump in its maximum penalties when aggravating factors are present. Using maximum penalties as a crude proxy for seriousness, one reasonable and unsurprising conclusion is that all twenty states surveyed take modifying data similarly seriously, at least with regards to attacks on government or critical infrastructure.

---

[142] *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).
[143] UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 272 note 2 (Russ.). For context, as of 2019, one million rubles is between fifteen and sixteen thousand U.S. dollars.
[144] STRAFGESETZBUCH [StGB] [PENAL CODE] § 303b (Ger.).
[145] *Id.* 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: Maximum Penalties for Modifying Data

| *State* | *Unauthorized modification of data (Months)* | *Unauthorized modification of data with aggravating factors (Months)* |
|---|---|---|
| Australia | 24 | 120 (or 60 to life, if done with intent to commit a subsequent offense) |
| Canada | 120 | --[146] |
| China | 60 | Minimum of 60 |
| Estonia | 36 | 60 |
| France | 36–60 | 60–120 |
| Germany | 24 | 36–120 |
| Iran | 6–24 | 36–120 |
| Israel | 36 | 36–60 |
| Japan | 60 | 84–120 |
| Netherlands | 24 | 36–60 |
| Oman | 12–36 | 36–120 |
| Russia | 4 (or 24 of labor) | 48–84 |
| Singapore | 36 | 84–120 |
| South Korea | 84 | 120 years |
| Spain | 6–36 | 24–60 |
| Sweden | 24 | 6 minimum to 72 maximum |
| Switzerland | 36 | 12–60 |
| Taiwan | 60 | 90 |
| United Kingdom | 120 | 120 to life |
| United States | 120 | 60 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.[147] But here, too, the United States is not alone.

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,

[146] *See supra* note 138.
[147] *See supra* Section II.B.2.

Israel, the United Kingdom, and the United States place the prohibition in their laws governing state wiretapping.[148] Canada, China, Singapore, South Korea, Switzerland, Taiwan, and the United States still sit at the high end of the spectrum (see Table 4).

Table 4: Maximum Penalties for Intercepting Data

| *State* | *Penalty for intercepting data in transit (Months)* |
|---|---|
| Australia | 24 |
| Canada | 60–120 |
| China | 36–84 |
| Estonia | (Fine only)[149] |
| France | 12 |
| Germany | 24 |
| Iran | 6–24 |
| Israel | 36 |
| Japan | 24 |
| Netherlands | 24 |
| Oman | 1–12 |
| Russia | 12– 24 |
| Singapore | 36–84 |
| South Korea | 60 |
| Spain | 3–24 |
| Sweden | 24 |
| Switzerland | 60 |
| Taiwan | 60 |
| United Kingdom | 24 |
| United States | 60 |

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.[150] France and

[148] 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. *See supra* Table 1. For a chart listing states with lawful intercept capability laws, see generally, Ian Brown, *Lawful Interception Capability Requirements*, SOC'Y FOR COMPUTERS & L. (Aug. 13, 2013), https://www.scl.org/articles/2878-lawful-interception-capability-requirements [https://perma.cc/2GEB-GE46].

[149] *See infra* note 156.

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

Japan stand out in being the only countries surveyed that penalize intercepting data in transit less severely than accessing data at rest.[151]

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.[152] That Act specifically prohibits third persons from intercepting information by means of radio equipment.[153] But neither the Electronic Communications Act nor the Penal Code contain a similar explicit prohibition on intercepting telecommunications made over the internet.[154]

Instead, Estonia has *constitutionalized* the right to confidential messages and prosecutes such activity under the general "Violation of confidentiality of messages" provision of the Penal Code.[155] But counterintuitively, that provision warrants only an *unspecified fine* in most circumstances.[156] Estonia's decision to be less specific in its penal prohibitions may reflect both a dedication to the free and open internet model and a preference for placing the cybersecurity liability burden squarely on telecommunications providers, while still complying with its

---

[151] 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.

[152] ELEKTROONILISE SIDE SEADUS (Electronic Communications Act) 2005, c. 10 (Est.), https://www.riigiteataja.ee/en/eli/501042015003/consolide [https://perma.cc/C3P3-NQUL].

[153] § 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 method "in which electromagnetic waves propagating in open space are used as the information carrier." *Id.* at § 22(44).

[154] *Id*.; *accord* KARISTUSSEADUSTIK (Penal Code), c. 13 (Est.), https://www.riigiteataja.ee/en/eli/ee/523122015005/consolide/current [https://perma.cc/6H6W-EHDK].

[155] EESTI VABARIIGI PÕHISEADUS (Constitution of the Republic of Estonia) 1992, § 43 (Est.) ("Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means."); KARISTUSSEADUSTIK (PENAL CODE), c. 13, § 156 (Est.) ("Violation of the confidentiality of a message communicated by a letter or other means of communication is punishable by a pecuniary punishment."); *see* Riigikohus [Supreme Court] Case # 3-1-1-93-15 (Est.) (stating that e-mails in transit are protected by § 43 of the Constitution and § 156 of the Penal Code) (in Estonian), https://www.riigiteataja.ee/kohtulahendid/detailid.html?id=206132572 [https://perma.cc/HQM8-GKZF]

[156] KARISTUSSEADUSTIK (PENAL CODE), c. 13, § 156 (Est.).

constitutional treaty obligations.[157] Estonia regulates internet content lightly, but telecommunications cybersecurity heavily.[158]

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.

Sections IV.E through IV.G, *supra*, 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. 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.[159] Laws of this type may be relevant, for example, in cases prosecuting perpetrators of denial-of-service attacks.

---

[157] 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 (Est.); *c.f.*, *Freedom on the Net 2017: Estonia Country Profile*, FREEDOM HOUSE, 2017, https://freedomhouse.org/report/freedom-net/2017/estonia [https://perma.cc/S37M-KKC5] (indicating that Estonia has one of the most lightly-regulated yet robust telecommunications industries in the world).

[158] Both the Electronic Communications Act, and the new Cybersecurity Act 2018 provide for significant state oversight of internet service providers' cybersecurity. *Supra* note 152; *accord* KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018 (Est.). For an overview of Estonian information technology laws and unique public-private structure, see generally Mihkel Miidla & Liisa Kuuskmaa, *Estonia*, 9 TECH., MEDIA & TELECOM. REV. (2019), https://thelawreviews.co.uk/edition/the-technology-media-and-telecommunications-review-edition-9/1177982/estonia [https://perma.cc/7Y7V-K9ZR]; Anna-Maria Osula, *National Cyber Security Organization: Estonia*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE REPORTS (2015), https://ccdcoe.org/uploads/2018/10/CS_organisation_ESTONIA_032015_1.pdf [https://perma.cc/J8MP-HXJJ].

[159] This phrasing, or a variation, appears in most criminal statutes or related treaties. *See, e.g.*, Budapest Convention, *supra* note 66.

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,[160] Spain,[161] and Taiwan[162] are the only three exceptions.

Table 5: Interference with Normal Computer Functions

| *State* | *Penalty (Months)* |
|---|---|
| Australia | 120 |
| Canada | 120 |
| China | 60 (the minimum for serious consequences) |
| Estonia | 36–60 |
| France | 60–84 |
| Germany | 36–120 |
| Iran | 6–24 |
| Israel | 36–60 |
| Japan | 36–60 |
| Netherlands | 24–60 |
| Oman | 24–36 |
| Russia | 24–60 |
| Singapore | 60–84 |
| South Korea | 50 |
| Spain | 6–36 (36–96 with aggravating factors) |
| Sweden | 6–72 |
| Switzerland | 36–60 |
| Taiwan | 36 |
| United Kingdom | 120 |
| United States | 12–240 |

[160] *Compare* MAJMUAHI QAVANINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1388 [2009], article 734 [9] (Iran) (declaring 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).

[161] *Compare* CÓDIGO PENAL [C.P.] [PENAL CODE] art. 264 bis (Spain), *with* art. 264 (declaring interference with normal computer functions and deletion of computer data as both punishable by a term of 6 months to 3 years).

[162] *Compare* Zhōnghuá mínguó xíngfǎ (中華民國刑法) [CRIMINAL CODE OF THE REPUBLIC OF CHINA] 1935, art. 359 (Taiwan) *with* art. 360 (declaring interference with normal computer functions as punishable by a term of 3 years while deletion of computer data is punishable by 5 years).

I. *Nuances in Laws Prohibiting the Trade in Programs*

No survey of computer crime laws would 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 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.[163] 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.[164] Under the terms of the Convention, state 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.[165]

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).[166] 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 parties transposed it into their domestic laws.[167]

Germany, for example, enacted STGB (Penal Code) § 202c in 2007. That section originally provided that:

---

[163] Budapest Convention, *supra* note 66, art. 6.
[164] Budapest Convention, *supra* note 66, art. 6.
[165] *See* Budapest Convention, *supra* note 66, art. 6.
[166] 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://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ [https://perma.cc/3Y4H-KL87].
[167] The international struggle to regulate the trade in computer programs that can be used by either white-hat or black-hat hackers continues to this day. *See, e.g.*, Shaun Waterman, *The Wassenaar Arrangement's Latest Language Is Making Security Researchers Very Happy*, CYBERSCOOP (Dec. 20, 2017), https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/ [https://perma.cc/DZ5K-AQZJ] (describing how language in the Wassenaar Arrangement arms-control treaty was modified in 2017 so that it would not apply to hacking tools used by cybersecurity researchers).

> Whosoever prepares the commission of an offence under section 202a [i.e., unauthorized access to restricted data at rest] or section 202b [i.e., 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.[168]

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 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.[169] Some cybersecurity companies stopped doing business in Germany;[170] 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.[171] Things calmed down after the Federal Constitutional Court ruled that STGB § 202c charges were inadmissible against Information Technology ("IT") professionals and academics who lacked the requisite intent to use the programs to commit crimes,[172] but the episode lives on as a cautionary tale of how the plain language of laws affects public behavior in rule-of-law cultures.[173]

---

[168] 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 an EU Directive. *See* Directive 2013/40, of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L 218), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF [https://perma.cc/8PWK-6BBP] (setting forth guidance—some hortatory, some prescriptive—for member state cybercrime laws).

[169] *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://www.tecchannel.de/a/das-bsi-und-der-hackerparagraf-202c-keine-strafverfolgung-durch-staatsanwalt,1737140 [https://perma.cc/JL2J-YBKH] (in German).

[170] *See German Security Professionals in the Mist*, SÛNNET BESKERMING COMMENTARY (Aug, 12, 2007), http://www.beskerming.com/commentary/2007/08/12/249/German_Security_Professionals_in_the_Mist [https://perma.cc/ER7H-2TR3] (listing German "security related products and groups [that] have either closed up shop or relocated to countries of convenience, such as the Netherlands").

[171] *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://www.heise.de/security/meldung/Hacker-Paragraf-iX-Chefredakteur-zeigt-sich-selbst-an-191403.html [https://perma.cc/7EAJ-FMMY] (in German).

[172] *See* BverfG (Federal Constitutional Court), 2 BvR 2233/07, May 18, 2009, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-067.html [https://perma.cc/6SPL-E6Q5] (in German).

[173] *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),

With the German story as illustrative 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.

https://archive.is/20130213112150/http:/www.jlussi.eu/2007/11/01/cybercrime-convention-german-criminal-law-it-security/#selection-45.1-45.15 [https://perma.cc/QP8Q-4JAD] (summarizing in English a "handle with care – but don't panic" presentation given at the 2007 Munich Information Security Summit before STGB § 202c came into effect; also explaining that German law does not criminalize abstract endangerments).

Table 6: Nuances in Hacking Tool Laws

| *State* | *Possession prohibited?* | *Trade prohibited?* | *Penalty? (Months)* | *Research exceptions or other relevant limiting language?* |
|---|---|---|---|---|
| Australia | Yes | Yes | 36 | Only prohibits possession or trade if done "with the intention that the data be used" to commit computer crimes |
| Canada | Yes | Yes | 120 | Only prohibits possession and trade "without lawful excuse" |
| China | Creation prohibited; possession not prohibited | Yes | 36–84 | 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 | 24 | Only prohibits programs designed "in particular for the commission of" computer crimes. |
| France | Yes | Yes | 60–84 | Only prohibits programs "specially adapted" to commit computer crimes<br>Research or computer security is an explicit exception |
| Germany | Yes | Yes | 24 | The Constitutional Court has treated the phrase "for the purpose of" as incorporating a specific intent element |
| Iran | No | Yes | 91 days – 12 months | Only prohibits trade in programs "exclusively used" to commit computer crimes |
| Israel | Creation prohibited; possession not prohibited | Yes | 36–60 | Prohibits trade in all programs "enable[d] to perform" computer crimes |
| Japan | Yes | Yes | 24–36 | 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 | 36–60 | Only prohibits possession or trade in programs "with the intention of using it in the commission of a serious offence" |
| Oman | Yes | Yes | 6–36 | 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 | 48–84 | Only prohibits creation/trade of programs "knowingly intended for" use in committing computer crimes |

| *State* | *Possession prohibited?* | *Trade prohibited?* | *Penalty? (Months)* | *Research exceptions or other relevant limiting language?* |
|---|---|---|---|---|
| Singapore | Yes | Yes | 36–60 | 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 | 84 | Only prohibits trade in programs "likely to interrupt operation" of a computer system |
| Spain | No | Yes | 6–24 | Only prohibits trade in programs with the intention to facilitate computer crime |
| Sweden | Only prohibited if done as a preparatory act[174] | -- | 24 | Neither possession nor trade is prohibited, unless done in preparation for a data breach |
| Switzerland | Creation prohibited; possession not prohibited | Yes | 36 | 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 | 60 | Only prohibits creation or trade in programs when done "specifically for himself or another to commit" a computer crime |
| United Kingdom | Creation prohibited; possession not prohibited | Yes | 24 | Prohibits creation of programs intended for use in committing computer crimes;<br><br>Prohibits trade in programs believing they are likely to be used to commit computer crimes |
| United States | Creation prohibited; possession of > 15 programs with intent to defraud also prohibited | Yes | 120–240 | Intent element: "knowingly and with intent to defraud"<br><br>In addition, computer code in the United States enjoys some degree of protection under the First Amendment to the U.S. Constitution.[175] |

[174] *See* Anders Hellström & Erik Myrberg, *Sweden: Cybersecurity 2019*, INTERNATIONAL COMPARATIVE LAW GUIDE (Oct. 16, 2018), https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/sweden [https://perma.cc/9GNJ-FW5N] (citing an unspecified Swedish Court of Appeal).

[175] *See, e.g.*, Bernstein v. U.S. Dept. of State, 922 F. Supp. 1426 (N.D. Cal. 1997); *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 United Kingdom, and the United States) prohibit creating such programs "with intent to commit computer crimes," or similar language, but do not prohibit possession per se. Three states (Iran, South Korea, and Spain) don't prohibit possession at all, proscribing 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 United Kingdom, and the United States) on the more permissive end of the spectrum.[176]

(2) By contrast, every state surveyed 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 "give unauthorized commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention."[177] 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 does not interfere with the normal operator's ability to access the data.[178]

(4) Every state surveyed has language or—for Germany and Sweden, case law—that clarifies the statute, making the prohibited possession or trade in such programs criminal only if done with intent to commit or facilitate an unlawful act. In a sense, this intent language implies a sphere of lawful activity.

(5) Yet no state, except France, has an explicit exception for programs used for research and security testing.[179] This does not necessarily mean that research

---

[176] Russia, the United Kingdom, and the United States are members of the recently modified Wassenaar Arrangement, while China, Iran, and Israel are not. *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Feb. 2017, https://www.wassenaar.org/about-us/ [https://perma.cc/2WMV-79BP].

[177] KEIHŌ (PEN. C.) 1907, art. 168-2 (Japan); *see also* Hayashi, *supra* note 105.

[178] KEIHŌ, *supra* note 177; *see also* Hayashi, *supra* note 105.

[179] CODE PENAL [C. PEN.] [Penal Code] art. 323-3-1 (Fr.); *see* CODE DES POSTES ET DES COMMUNICATIONS ELECTRONIQUES [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 also* 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 Dec. 18, 2013 on military programming for the years 2014 to 2019 and containing various

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, "[i]n comparison to other federal crimes, CFAA offenses are not charged frequently – and prosecuting someone engaged [sic] computer security research is *extraordinarily rare*."[180] Still, as the German example suggests, a law that facially prohibits such programs and requires cybersecurity professionals to rely on prosecutorial discretion rather than an explicit legal defense can have a chilling effect.

Taken together, these points suggest it is not by chance that, at least by one ranking, the most innovative cybersecurity companies in the world are clustered in a handful of states, of which all but Canada clearly take relatively permissive official attitudes toward the possession of computer programs: the United States, Israel, the United Kingdom, Canada, France, Sweden, and China.[181]

J. *Other Relevant Laws*

Other laws may be at least tangentially relevant to private-sector actors considering active defense measures. 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.[182] Notably, Australia, Canada, and China also permit ISPs (but not other companies) to take affirmative protective measures on their own.

---

provisions concerning defense and national security], art. 25 (Dec. 20, 2018), https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1E40D565ADF26DEF442B58CA4E3E59A1.tplgfr36s_2?cidTexte=JORFTEXT000028338825&idArticle=LEGIARTI000028340498&dateTexte=20131220 [https://perma.cc/L38C-NV8A].

[180] *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://www.blackhat.com/docs/us-15/materials/us-15-Bailey-Take-A-Hacker-To-Work%20Day-How-Federal-Prosecutors-Use-The-CFAA.pdf [https://perma.cc/2F2T-XVDZ] (emphasis in original). In fiscal year 2017, for example, U.S. Attorneys brought 165 cases that included charges under the CFAA. *U.S. Attorneys' Annual Statistical Report Fiscal Year 2017*, U.S. DEPARTMENT OF JUSTICE, Table 3B, https://www.justice.gov/usao/page/file/1081801/download [https://perma.cc/FJ9N-XE67]. To focus on a particular example from 2013–14, see generally Jordan Robertson & Michael Riley, *Would the U.S. Really Crack Down on Companies that Hack Back?*, BLOOMBERG (Dec. 30, 2014), https://web.archive.org/web/20160317041319/https://www.bloomberg.com/news/2014-12-30/why-would-the-u-s-crack-down-on-companies-that-hack-back-.html [https://perma.cc/M6YN-M4WV]; Michael Riley & Jordan Robertson, *FBI Probes If Banks Hacked Back as Firms Mull Offensives*, BLOOMBERG (Dec. 30, 2014), https://web.archive.org/web/20190716042555/https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives [https://perma.cc/ELR9-7YHZ] (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).

[181] *See supra* note 79. Why Canada has so many cybersecurity companies, despite its consistently strict penalties and broad statutory prohibitions, is a good question for future research.

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

Specifically, Australia permits an ISP to trace any person "suspected of a violation" of the computer crimes discussed in this Article.[183] 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 discussed here]."[184] China criminalizes an ISP's failure to protect its network if it fails to comply with basic security requirements, as defined by regulation.[185]

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.[186] In Estonia and South Korea, ISPs must monitor their networks (but are 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

[183] "[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.).

[184] Canada Criminal Code, R.S.C. 1985, c C-46, art. 184(2)(e) (Can.) ("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].").

[185] 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. The ninth amendment has not been formally translated into English but scholars have provided informal translations. *See* Jeremy Daum, *It's a crime, I tell ya: Major Changes in China's Criminal Law Amendment 9,* CHINA LAW TRANSLATE (Sept. 27, 2015), https://www.chinalawtranslate.com/en/its-a-crime-i-tell-ya-major-changes-in-chinas-criminal-law-ammendment-9/ [https://perma.cc/J7VY-6NRN].

[186] CODE DES POSTES ET DES COMMUNICATIONS ELECTRONIQUES [Post and Electronic Communications Code], arts. 33-14 & 34-1 (Fr.) ("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*, [] devices implementing technical markers solely for the purpose of detecting events likely to affect the security of the information systems of their subscribers.") (emphasis added).

activity to the state.[187] In Estonia,[188] Singapore,[189] and South Korea,[190] the state has the power to direct the ISP's defenses. By contrast, Japanese law requires ISPs to restrict their responses to basic public-private information sharing.[191]

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.[192]

---

[187] KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018, c. 2 § 7 (Est.); *accord* Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. [Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016, art. 48-2 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do ("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.").

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

[189] *See* Computer Misuse Act 1993, *supra* note 106.

[190] 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 [state] may, if necessary to take countermeasures against intrusion, request [that ISPs] provide human resources for assistance.").

[191] Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Law No. 128 of 1999, arts. 8–10, translated in (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp (Japan) (encouraging ISPs and network administrators to harden internal network defenses and public-private information sharing).

[192] *See, e.g.*, MAJMUAHI QAVANINI JAZAI [CODE OF CRIMINAL LAWS] Tehran 1381 [2002], arts. 744–745 (Iran); Royal Decree No. 12/11, Issuing the Cyber Crime Law, Article 29 (Oman); Penal Code Arts. 197, 264 (Spain). There is no obvious distinction in either substance or organization between the laws of Budapest states parties and non-states parties. *C.f.* Budapest Convention, *supra* note 66, art. 12 (calling states parties to establish provisions for corporate liability).

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. |
| 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 known. *But contemplated, see Section IV.D.3.* |
| 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.<br>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. |

| *State* | *Any other laws relevant to active defense measures?* |
|---|---|
| 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. |
| United Kingdom | 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. |
| United States | *Contemplated, see Section IV.D.3, supra*. |

## V. Conclusion

This Article focuses on description rather than on normative theories. The normative space is crowded and the descriptive space relatively unoccupied. But the law on the books provides essential groundwork for the normative arguments—perhaps even more so if the law on the books does not always reflect reality. It is difficult to determine which ideas are worth exploring without knowing what the law says, what is common, and what is rare.

Five basic conclusions bear on the future of the U.S.-based discussion around active defense measures.

First, 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 a better way to identify conduct that should be prohibited. Cyberspace is not a lawless Wild West.[193] Rather, it is teeming with law, and with few exceptions, that law is not 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."[194] But today, we hear little silence. U.S. private sector actors should be cautious of taking action that could 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 United States does. As Rosenzweig points out, although the United States is

[193] This point is not new, but is underscored for emphasis. *See also* Joseph S. Nye, Jr., *Cyber Power*, BELFER CENTER ESSAY 14 (2010), https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [https://perma.cc/8CXC-C6BZ].
[194] Rosenzweig, *supra* note 5, at 114.

unlikely ever to extradite a U.S. person to an adversary state, it would be harder to dismiss an appropriately couched extradition request from, say, Germany, Japan, Taiwan, or Israel.[195] There is no reason to believe that the passage of time will thin out rather than thicken these laws around the world.

Second, while not overt, it might be fair to label some of the twenty states sampled as *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 do not bar mere access to data at rest.[196] Six more do, but have relatively low maximum penalties (i.e., two years or less).[197] Only six states, including the United States, 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.[198] 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.[199] Rather, those states—among the fourteen mentioned above—may simply wish to make clear in their laws which types of activity they deem important and which they do not.

Third, and in contrast, Canada, China, South Korea, and the United States have clearly and consistently higher penalties on the books than other states. Yet, the DOJ, for example, has told hacker conferences that they are unlikely to pursue low-level crimes (definition unclear) or security researchers.[200] In addition, a significant portion of the cybersecurity companies of the world have clustered in these countries, despite how strict their laws appear.[201] One logical question for future research would look more deeply at whether a permissive "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.[202]

Fourth, mapping out the landscape brings into relief interesting details, otherwise difficult to see. Of the states surveyed here, Australia's laws are by far the most detailed, lengthy, and granular. Sweden's are shortest. Yet, 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.[203] There are surprising oddities, like France's and Japan's decision to penalize intercepting data in transit less severely than accessing data at rest, or Estonia's

---

[195] *See* Rosenzweig, *supra* note 5, at 115.
[196] *See supra* Table 2.
[197] *See supra* Table 2.
[198] *See supra* Tables 2–5.
[199] *See supra* Tables 2–5.
[200] *See* Bailey Presentation, *supra* note 180.
[201] *See Cybersecurity 500 by the Numbers: Breakdown by Region*, *supra* note 79.
[202] *See* Rosenzweig, *supra* note 5, at 115.
[203] *See, e.g.*, KEIHŌ, *supra* note 140.

decision to constitutionalize communications privacy but punish violations with just a fine.[204] This overview cannot 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 identifies where the differences *are* and, as a policy matter, which ideas might be worth exploring further.

Finally, this research makes clear how rare it is for a country to contemplate loosening rules for private sector active defense measures. That is not to say that the United States should not do something just because it would be an outlier—it is often an outlier. But any effort to legalize private sector active defense in the United States will be of limited use without a broader international agreement among nations.

[204] *See supra* Section IV.G; *supra* Table 4.

# Appendix—Relevant Domestic Laws

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

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

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

For states whose governments do not publish English translations online, permalinks to the most reputable up-to-date source are provided. Translated excerpts of one Israeli law and one Russian article are provided here due to the difficulty involved in finding them online.

## I. [Commonwealth of] Australia

*Criminal Code Act 1995* (Cth) ch 10 pt 7 divs 476–78 (Austl.), https://www.legislation.gov.au/Details/C2019C00043/Html/Volume_2#_Toc535487479 [https://perma.cc/L2H4-3ETP].

*Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2.1, 2.9 (Austl.), https://www.legislation.gov.au/Details/C2019C00010 [https://perma.cc/N7TB-PEJM].

## II. Canada

Canada Criminal Code, R.S.C. 1985, c C-46, https://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html [https://perma.cc/Z2EE-V3XS].

## III. [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, July 1, 1979) (Ninth Amendment promulgated by the Standing Committee of the Second National People's Congress, Aug. 29, 2015, effective Nov. 1, 2015), arts. 283–87 (China).

The most recent English translation includes only Amendments 1–8. Criminal Law of the People's Republic of China, CONGR.-EXECUTIVE COMMISSION ON CHINA,

https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china [https://perma.cc/UQT8-7BMW].

The 9th Amendment (2015) amended: (1) Articles 283–86 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 287 bis) 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. *Ninth Amendment to the Criminal Law of the People's Republic of China*, CONGR.-EXECUTIVE COMMISSION ON CHINA, https://www.cecc.gov/resources/legal-provisions/ninth-amendment-to-the-criminal-law-of-the-peoples-republic-of-china [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 L. TRANSLATE BLOG (Sept. 27, 2015), https://www.chinalawtranslate.com/en/its-a-crime-i-tell-ya-major-changes-in-chinas-criminal-law-ammendment-9/ [https://perma.cc/4P2T-B5UB].

IV. [Republic of] Estonia

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://www.president.ee/en/republic-of-estonia/the-constitution/ [https://perma.cc/J3YF-PC99].

KARISTUSSEADUSTIK (Penal Code), c. 13 (Est.), https://www.riigiteataja.ee/en/eli/ee/523122015005/consolide/current [https://perma.cc/6H6W-EHDK].

ELEKTROONILISE SIDE SEADUS (Electronic Communications Act) 2005, c. 10 (Est.), https://www.riigiteataja.ee/en/eli/501042015003/consolide [https://perma.cc/C3P3-NQUL].

KÜBERTURVALISUSE SEADUS (Cybersecurity Act) 2018 (Est.), https://www.riigiteataja.ee/en/eli/523052018003/consolide [https://perma.cc/YY2H-UQ2A].

V. France [French Republic]

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. 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. *Penal Code*, LEGIFRANCE (DEC. 10, 2005), https://www.legifrance.gouv.fr/affichCode.do;jsessionid=52C55706BDE60C65FE9D214BC6224824.tplgfr36s_2?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20190329 [https://perma.cc/6LW8-GRZV].

CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [CRIMINAL PROCEDURE CODE], art. 706-102 (Fr.), https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000023712497&dateTexte=&categorieLien=cid [https://perma.cc/HYG6-YJZ7] (governing state oversight of interception).

CODE DES POSTES ET DES COMMUNICATIONS ÉLECTRONIQUES [POST AND ELECTRONIC COMMUNICATIONS CODE], arts. 33-14 & 34-1 (Fr.), https://www.legifrance.gouv.fr/affichCode.do;jsessionid=D28B02B8D2676C6A030CC9F66F6FB794.tplgfr36s_2?idSectionTA=LEGISCTA000006165902&cidTexte=LEGITEXT000006070987&dateTexte=20190402 [https://perma.cc/Y2KX-A7ED] & https://www.legifrance.gouv.fr/affichCode.do;jsessionid=D28B02B8D2676C6A030CC9F66F6FB794.tplgfr36s_2?idSectionTA=LEGISCTA000006165910&cidTexte=LEGITEXT000006070987&dateTexte=20190402 [https://perma.cc/52QM-WR84] (governing exceptions to Art. 323 of the Penal Code).

VI. [Federal Republic of] Germany

STRAFGESETZBUCH [STGB] [PENAL CODE] (Ger.).

The most recent English translation is from 2013, *German Criminal Code*, BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHTUZ, https://www.gesetze-im-internet.de/englisch_stgb/ [https://perma.cc/9ZVR-X4LJ].

Amendments since 2013 increased the penalty in § 202c and added subparagraph (3) to § 303a. Strafgesetzbuch (StGB), BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHTUZ, https://www.gesetze-im-internet.de/stgb/BJNR001270871.html [https://perma.cc/EYQ3-X6MK].

VII. [Islamic Republic of] Iran

MAJMUAHI QAVANINI 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 *Computer Crimes Act*, CYBER POLICE ISLAMIC REPUBLIC OF IRAN (Sept. 3 2014), https://sherloc.unodc.org/res/cld/document/computer-crimes-act_html/Computer_Crimes_Act.pdf [https://perma.cc/8SJK-XSGG]; *see also Cyber Law*, CYBER POLICE ISLAMIC REPUBLIC OF IRAN, http://cyber.police.ir./ [https://perma.cc/76M4-B2EN]. 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 Article, both the Code number and the Act number, following in brackets, are provided.

VIII. [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). This Article uses a 2015 translation from Aryeh Greenfield Publications (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 aligns with the A.G. Pub. translation is held by the UNODC. However, this version does not include citation or translation information. *Computers Law, 1995*, UNITED NATIONS OFF. ON DRUGS AND CRIME, https://www.unodc.org/res/cld/document/computer-law_html/Israel_Computers_Law_5755_1995.pdf [https://perma.cc/N9LK-Q9E6].

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

There is no readily-available internet source for this law in English, although the law itself is publicly available in LSI hard copy. The official translation provides:
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.

IX. Japan

KEIHŌ [PEN. C.] 1907 (Japan), *translated in* (Japanese Law Translation [JLT DS]), https://www.japaneselawtranslation.go.jp [https://perma.cc/5LKW-U6J7].

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

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

X. [Kingdom of the] Netherlands

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

The most recent English translation is from 2012. *Criminal Code*, EUR. JUD. TRAINING NETWORK, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf [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 (Criminal Code) (SR) (Neth.), https://wetten.overheid.nl/jci1.3:c:BWBR0001854&z=2019-03-01&g=2019-03-01.

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 Article. *See Staatsblad van het Koninkrijk der Nederlanden*, EERSTE KAMER DER STATEN-GENERAAL (2018), https://www.eerstekamer.nl/behandeling/20180921/publicatie_wet/document3/f=/vkrxd3beqlvv.pdf [https://perma.cc/DL7K-HYFN] (in Dutch).

XI. [Sultanate of] Oman

Royal Decree No. 12/2011 [Issuing the Cyber Crime Law] [2011] (Oman), https://www.ita.gov.om/ITAPortal/Data/English/DocLibrary/FID2011411757466 6/Royal%20Decree%20No%20122011%20-

%20Issuing%20the%20Cyber%20Crime%20Law.pdf [https://perma.cc/ZK5V-Z83Z].

XII. 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. *The Criminal Code of the Russian Federation*, WORLD INT'L PROP. ORG. (June 13, 1996), https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf [https://perma.cc/TF3D-TSAA].

Key amendments since 2012 include the addition of new 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. *The Criminal Code of the Russian Federation*, UNITED NATIONS OFF. ON DRUGS AND CRIME (June 13, 1996), https://sherloc.unodc.org/res/cld/document/criminal-code-of-russian-federation-russian_html/_13.06.1996_N_63-.rtf [https://perma.cc/EV7K-XBE4]. Russian text is 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, an unofficial translation is provided 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.

XIII. [Republic of] Singapore

Computer Misuse Act 1993, c. 50A § 1–9 (Sing.), https://sso.agc.gov.sg/Act/CMA1993 [https://perma.cc/4WGF-9Y58].

Cybersecurity Act 2018, § 23 (Sing.), https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&ViewType=Pdf&_=20180904203749 [https://perma.cc/XKC6-3US9].

XIV. South Korea [Republic of Korea]

Criminal Act, Act No. 293, Sept. 18, 1953, *amended by* Act No. 14415, Dec. 20, 2016 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do [https://perma.cc/WDV4-R7YJ]. Not cited in the paper, 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. [Network Act], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 14080, Mar. 22, 2016 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do [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 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/eng_service/main.do [https://perma.cc/9EN9-3JB8].

XV. [Kingdom of] Spain

CÓDIGO PENAL [C.P.] [Criminal Code] (Spain), https://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=038_Codigo_Penal_y_legislacion_complementaria.pdf [https://perma.cc/YBX7-93G3].

XVI. [Kingdom of] Sweden

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

The most recent English translation is from 1999. *The Penal Code*, GOV'T OFF. OF SWEDEN, https://www.government.se/49cd60/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf [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. Brottsbalk, Sveriges Riksdag, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700 [https://perma.cc/VEM6-MZS6].

XVII. Switzerland [Swiss Confederation]

SCHWEIZERISCHES STRAFGESETZBUCH [StGB] [CRIMINAL CODE] Dec. 21, 1937, SR 757 (1938), arts. 143–47 (Switz.), https://www.admin.ch/opc/en/classified-compilation/19370083/index.html [https://perma.cc/PVU8-YHXD].

XVIII. Taiwan [Republic of China]

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

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

XIX. United Kingdom [of Great Britain and Northern Ireland]

Computer Misuse Act 1990, c. 18, §§ 1–3 (UK), https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf [https://perma.cc/5V2W-R2DV].

Investigatory Powers Act 2016, c. 25, § 3 (UK), https://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf [https://perma.cc/X8AA-X57L].

XX. United States [of America]

18 U.S.C. § 1030 (2018) (Computer Fraud and Abuse Act (CFAA))

18 U.S.C. § 2510–2522 (2018) (Wiretap Act)

18 U.S.C. § 3121 (2018) (prohibition on pen register/trap and trace devices)