Notes

Botnet Mitigation and International Law

Columbia Journal of Transnational Law Student Writing Prize in Comparative and International Law, Best Note Award

Advances in technology have outpaced development of laws governing cyberspace, leading, at times, to a wild-west law enforcement regime. And in a world of Botnets—massive armies of unknowingly conscripted systems directed by anonymized 'botmasters'—domestic criminal law is no longer a sufficient response to cyberthreats.

States now act against a backdrop of international animus over what many nations see as surveillance overreach by the United States and Five Eyes partners who enjoy an overbroad grant of executive discretion, capture data indiscriminately, and operate in relative secrecy.

This Note outlines the various technologies employed by outlaw and government actors. It describes how these technologies confound territorial limitations on enforcement jurisdiction in international law. It discusses advances in botnet-disruption methods by private and government actors and how nations wishing to constrain powerful western intelligence agencies have reached to pre-cyber human rights and privacy law as a response to perceived surveillance overreach. This Note describes technical elements of recent U.S. Department of Defense anti-botnet efforts and how they may or may not implicate surveillance

law. It explains that rather than vague legal barriers, nations need laws authorizing good-faith enforcement by cyber-capable states and procedural norms that guide development of technological solutions that operate consistently with universal values. Finally, it outlines promising sources of international law developing around this issue and advocates for development of a mutually recognized state duty to disrupt cybercriminals and expanded cooperation between nations in botnet disruption.

INTRODUCTION

Comparisons between data and oil or gold are so common that they have become hackneyed in business media.[1] While both criminal and legitimate actions in cyberspace have grown around the increased value of data, they have done so asymmetrically due to uneven limitations: while criminal enterprises are constrained only by capability, law enforcement must also develop new legal instruments authorizing enforcement actions, many of which involve the monitoring or alteration of private data.

Botnets are an apex species in the cybercrime ecosystem. They cost little to create, can be controlled from any physical location by unsophisticated individuals or sophisticated nation states alike, and enable a variety of devastating attacks suitable to a diverse array of targets.[2] Botnet mitigation developed in response, beginning with private parties acting on their own, adopting both vigilante and governmental aspects. As private-sector actors—often directly threatened by botnet-enabled crime—pioneered anti-botnet interdiction methods, U.S. law enforcement delegated authority to employ active measures against their attackers, creating a private-public partnership, which has operated with increasing efficiency.

As botnet-enabled cyberattacks have become more transnational in scope, blurring territorial boundaries in cyberspace, what limitations extant international law will place on management remains uncertain. Nations wishing to constrain others' enforcement regimes will likely reach for vague and unwieldy tools in human rights and privacy law. Meanwhile, nations driving responses to bot-

1. *See, e.g.*, Sam Abuelsamid, *Like Mining Gold, Extracting Data Value Takes Effort*, FORBES (Oct. 5, 2018), https://www.forbes.com/sites/pikeresearch/2018/10/05/like-mining-gold-extracting-data-value-takes-effort/#610f7afb5260 [https://perma.cc/Z3EH-TRM6]; Bernard Marr, *Here's Why Data Is Not the New Oil*, FORBES (Mar. 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#2ab3cc7a3aa9 [https://perma.cc/JF2Z-4BQ6]; Robert Peck, *Mark Cuban: "Data Is the New Gold"*, CREDIT SUISSE GROUP (June 22, 2017), https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/mark-cuban-data-is-the-new-gold-201706.html [https://perma.cc/H2QN-38A9]; Arvind Singh, *Is Big Data the New Black Gold?*, WIRED (Feb. 2013), https://www.wired.com/insights/2013/02/is-big-data-the-new-black-gold/ [https://perma.cc/6E8D-F8WK]; Naser Tamimi, *Data Is Not Gold. Data Is Not Oil.*, MEDIUM CORPORATION (Sept. 28, 2018), https://medium.com/datadriveninvestor/data-is-not-gold-data-is-not-oil-9878ad28d12b [https://perma.cc/E2G6-8BCR]. *The World's Most Valuable Resource Is no Longer Oil but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/BHT5-ULPB].

2. *See* discussion *infra* Sections I.A, I.B.

nets must guess what laws will describe the boundaries of their actions. Against this backdrop, states have begun to coalesce around both norms-driven and binding legal structures built to guide technological innovation and cyber-defense.

The community of nations should encourage these latter developments, which offer governments guidance in designing responsive enforcement mechanisms, promise a uniform baseline of criminalization of these activities, and encourage information sharing—allowing enforcement operations to be conducted without the secrecy attendant to the adjacent field of signals surveillance. This Note describes the actors, technologies, and laws at play in emergent crime management in cyberspace and the less- and more-functional legal responses developing in international law. First, it explains how botnets operate. Second, it discusses the trajectory of botnet-mitigation techniques—from an early 'wild west' approach to an increasing occupation by sophisticated government actors. Third, it explains how some have proposed pre-cyber fields of law as a response to governmental involvement in transnational communications, and how these laws are poorly suited in light of technological developments. Finally, it describes emerging legal approaches to the issue: (a) the application of vague human rights and pre-cyber privacy law that offers little guidance to security practitioners who want to protect investments in cyberspace without violating international law or deterring potential partners and (b) a framework of negotiated procedural norms, mechanisms for harmonizing substantive law, and a negotiated duty to act against cyberthreats.

I. THE BOTNET PROBLEM

A. What Are Botnets?

Botnets enable a broad set of novel crimes—making them chief among emergent tools available to cybercriminals.[3] Botnets consist of unsuspecting, non-malicious internet-connected devices acting, without their owners' knowledge, toward a common purpose,

3. Adeeb Alhomoud et al., *A Next-Generation Approach to Combating Botnets*, 46 COMPUTER 62, 62 (2013) ("Cybercrime has become the most lucrative global criminal activity, costing businesses, governments and consumers an estimated $114 billion annually.") (citing *Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre*, COM (2012) 140 (Mar. 28, 2012), *available at* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF [https://perma.cc/6L8Y-28AS]).

as dictated by a botmaster.[4] To gain control of these computers, command-and-control ("C&C") servers distribute malware,[5] called the bot binary, to systems which in turn infect other systems. This covert "viral" infection method allows "exponential-like" growth of the botnet army while limiting markers that might identify the C&C location.[6]

In the first instance, vulnerable systems can be infected in many ways. These include phishing—sending fraudulent emails that redirect users to malicious websites—and remotely scanning[7] for vulnerable computers, servers, or even internet of things ("IoT") devices,[8] which are then penetrated using brute force or dictionary attacks,[9] social engineering, or infected media devices such as U.S.B.

4. Neamen Negash & Xiangdong Che, *An Overview of Modern Botnets*, 24 INFO. SECURITY J.: A GLOBAL PERSPECTIVE 127, 127 (2015).

5. *Id.* at 129.

6. Moheeb Abu Rajab et al. call this an "exponential-like growth pattern." The growth-rate increases as a function of time based on the ability of new bots to propagate. Moheeb Abu Rajab et al., A MULTIFACETED APPROACH TO UNDERSTANDING THE BOTNET PHENOMENON, *in* PROCEEDINGS OF THE 6TH ACM SIG-COMM ON INTERNET MEASUREMENT (IMG) 41, 47 (2006). They must first contact the C&C server and receive an instruction to do so. *Id.*; *see also* Manos Antonakakis et al., *Understanding the Mirai Botnet*, 26 USENIX SECURITY SYMPOSIUM 1092, 1097–98, 1098 figs. 3 & 4 (2017) (explaining how the Mirai botnet grew over time). Botnet networks can grow at an alarming rate, but the growth peaks and dips before reaching a steady-state. *Id.* at 1098–99. This Note uses the C&C botnet framework for instructive purposes only. Peer-to-peer botnet architecture is not addressed, not because it is not a significant threat but because the difference does not bear on the conclusions this Note draws.

7. Rajab et al., *supra* note 6, at 46 ("Scanning is by far the most prevalent spreading mechanism.").

8. *See* Antonakakis et al., *supra* note 6, at 1093–94 (describing how the Mirai botnet functions by preying on weaknesses inherent to internet-of-things devices). Internet of things is a colloquial term for smart, internet-connected devices including televisions, wi-fi routers, lightbulbs, washing machines, etc. *See also* Steve Ranger, *What is the IoT? Everything You Need to Know About the Internet of Things Right Now*, ZDNET (Aug. 21, 2018), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ [https://perma.cc/2WF8-GTS3].

9. *See* Antonakakis et al., *supra* note 6, at 1094, 1106 ("If Mirai identifies [*sic*] a potential victim, it entered into a brute-force login phase in which it attempted to establish a Telnet connection using 10 username and password pairs selected randomly from a pre-configured list of 62 credentials.") ("The Mirai botnet demonstrated that even an unsophisticated dictionary attack could compromise hundreds of thousands of Internet-connected devices."); Constantinos Kolias et al., *DDoS in the IoT: Mirai and Other Botnets*, 50.7 COMPUTER 80, 80–81 (July 2017) (The Mirai botnet "deduces the administrative credentials of other IoT devices by means of brute force, relying on a small dictionary of potential username–password pairs."). *See also* Mudassar Raza et al., *A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication*, 19 WORLD

flash drives. Once a device is penetrated, the binary will execute, attempt to secure itself within the device,[10] contact a Domain Name System (DNS) server to locate the C&C server, and potentially attempt to further penetrate any system to which the device is attached.

A bot's activity before an attack is difficult to distinguish from innocuous internet activity. Once a system is infected with a botnet's binary, it communicates with an independent DNS server to resolve the C&C server's internet protocol (IP) address.[11] Once it does, it can connect to the C&C server, download updated binaries, and receive orders from the botmaster.[12]

The paradigmatic botnet-enabled crime is the distributed denial of service attack ("DDoS").[13] In a DDoS, each bot will simultaneously and repeatedly send queries to a target server, overwhelming the server's data processing capacity and rendering it nonoperational. Botmasters execute DDoS attacks for a number of reasons. They are

APPLIED SCI. J. 439 (2012) for a primer on popular methods of circumventing systems security, not all of which apply, here.

10. Botnet malware will often alter its system's outward-facing behavior to protect itself from monitoring or attempts to neutralize it. Negash & Che, *supra* note 4, at 129. Furthermore, botnets will engage in a defensive maneuver known as "domain flux" whereby the C&C's domain name changes according to an algorithm it shares with malware-infected systems. In this way, anyone without the algorithm is unable to map the botnet's labyrinthine network. Lately, researchers and responders have used machine and deep learning techniques to fingerprint domains in flux by analyzing traffic data. *See, e.g.*, Amine Boukhtouta et al., *Towards Fingerprinting Malicious Traffic*, 19 PROCEDIA COMPUTER SCI. 548 (2013); Bin Yu et al., Semi-Supervised Time Series Modeling for Real-Time Flux Domain Detection on Passive DNS Traffic, *in* MACHINE LEARNING AND DATA MINING IN PATTERN RECOGNITION 258 (Petra Perner ed., 2014). *See also* discussion *infra* note 81.

11. This is a very common query. A user instructs a computer to visit "www.YouTube.com," and, in order to comply, the computer must query a DNS server to find the specific IP address of the YouTube server. In this way, the DNS server acts as an address book. Meanwhile, the C&C server's address is liable to change at any time. *See* Xuan Dau Hoang & Quynh Chi Nguyen, *Botnet Detection Based on Machine Learning Techniques Using DNS Query Data*, 10 FUTURE INTERNET 43 (2018).

12. *See* Negash & Che, *supra* note 4, at 129.

13. Other unlawful activity includes the appropriation of privately-owned systems for: cryptocurrency mining, see Conner Forrest, *Nasty Botnet Uses WannaCry Exploit to Mine Cryptocurrency from Your Servers*, TECHREPUBLIC (Feb. 1, 2018), https://www.techrepublic.com/article/nasty-botnet-uses-wannacry-exploit-to-mine-cryptocurrency-from-your-servers/ [https://perma.cc/GY4U-QZCG]; cryptocurrency theft, see David Pan, *Hackers Launch Widespread Botnet Attack on Crypto Wallets Using Cheap Russian Malware*, COINDESK (Oct. 4, 2019), https://www.coindesk.com/hackers-launch-widespread-botnet-attack-on-crypto-wallets-using-cheap-russian-malware [https://perma.cc/E8LA-YX9K]; honeypot-aware botnets; advertising fraud; camera data theft; and extortion, see Antonakakis et al., *supra* note 6, at 1094.

commonly performed for small-scale harassment, to make a point about a pet issue, or as a show of force meant to impress the community.[14]

DDoS attacks can also do immense harm to businesses of all types. In its 2018 report, Neustar, an information security firm, reported that approximately eighty-four percent of the 1,010 companies in its study reported having been the target of at least one DDoS attack in the previous twelve months.[15] Eighty-six percent of that group claimed to have been targeted more than once.[16] Sixty-three percent of targeted companies reported peak hourly financial losses of at least $100,000 per hour of DDoS, and forty-three percent estimated peak losses at greater than $250,000 per hour.[17] The damage from these attacks can take the form of lost income or productivity from being offline, stolen property, liability for associated breaches of protected information (e.g., bank account information), reputational harms, or ransoms in the event of a ransomware attack.[18]

B. The Mirai Botnet: A Case Study

The Mirai botnet, generally considered the most threatening iteration of the tool, consists of a steady state of approximately 200,000 to 300,000 internet of things ("IoT") devices.[19] These include DVRs, wireless routers, imbedded device cameras, light-

14. Elie Burzstein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, CLOUDFLARE BLOG (Dec. 14, 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [https://perma.cc/5S9N-CZLW]. A controller targeted Brian Krebs' website, Krebs on Security, a popular blog, where he exposes cybercriminals. By his own count, Krebs was the target of 269 DDoS attacks between July 2012 and September 2016. *Id.* The Mirai attacks were the most powerful DDoS attacks recorded as of this Note's publication. The Mirai attack on Krebs was more than twice the volume of the second-largest attack on his online security service, prompting his site security provider to drop him as a client. *Id.* In response to this attack, Mr. Krebs wrote a well-known blogpost about the potential anti-speech harm that botnets threaten. *See* Brian Krebs, *The Democratization of Censorship*, KREBS ON SECURITY (Sept. 16, 2016), https://krebsonsecurity.
com/2016/09/the-democratization-of-censorship/ [https://perma.cc/85LX-F3SW].

15. Charlie Osborne, *The Average DDoS Attack Cost for Businesses Rises to Over $2.5 Million*, ZDNET (May 2, 2017), https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/ **[**https://perma.cc/R66Y-FK3G].

16. *Id.*

17. *Id.*

18. Mieke Eoyang et al., To Catch a Hacker 1, 4, 5–6, 12 (2018).

19. Antonakakis et al., *supra* note 6, at 1098.

bulbs—any sort of "smart" technology.[20] These devices share certain vulnerabilities[21] that make them ripe for exploitation: they come equipped with weak default passwords that people neglect to change, they are generally always on, and they rarely have an auto-update feature by which they secure themselves against emergent threats.[22]

We know who was behind the creation of the Mirai botnet.[23] The three young men—each between the ages of eighteen and twenty at the time of Mirai's deployment—confessed to violations of the Computer Fraud and Abuse Act in federal court in Alaska.[24] They were sentenced to five years of probation and 2,500 hours of community service, to be satisfied by their ongoing assistance with F.B.I. cyber enforcement.[25]

The Mirai case shows that traditional intervention may have little effect on the ongoing threat a botnet poses.[26] It is unlikely that much of the disastrous impact of the Mirai botnet can be directly attributed to the young men who created it. While they originally created the device to harass rival Minecraft players by attacking the servers on which they played,[27] more serious criminals quickly took hold of the technology and deployed it against both large- and small-scale targets.[28]

The 15,000 documented attacks attributable to Mirai and its

20. *Id.* at 1093.

21. The Government Accountability Office defines "vulnerability" as "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by an attacker." U.S. GOV'T ACCOUNTABILITY OFFICE, DATA PROTECTION: ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 4 n.4 (2018).

22. Antonakakis et al., *supra* note 6, at 1108.

23. Garrett M. Graff, *The Mirai Botnet Architects Are Now Fighting Crime with the FBI*, WIRED (Sept. 18, 2010), https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing/ [https://perma.cc/K24Y-2KC8].

24. Press Release, U.S. Dep't of Justice, Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybercrime Investigations (Sept. 18, 2018), https://www.justice.gov/usao-ak/pr/hackers-cooperation-fbi-leads-substantial-assistance-other-complex-cybercrime [https://perma.cc/QXZ7-QESE].

25. *Id.*

26. *See* Bursztein, *supra* note 14.

27. *Id.*

28. *See* Antonakakis et al., *supra* note 6. A group of researchers representing Google, Cloudflare, Akamai Technologies, the Merit Network, Georgia Institute of Technology, University of Michigan, and University of Illinois Urbana-Champaign published an extensive study of the Mirai botnet in which they documented over 15,000 attacks attributable to a number of botmasters.

near variants in less than a year and the authors' likely non-involvement with these attacks[29] are instructive in a law-enforcement context. Botnet management requires specific focus on the tools of the crimes rather than the individual creators of the bots. Management can be achieved by keeping the magnitude of a DDoS below the breakpoint of a target server's processing capacity, which results in little, if any, damage. A combination of information-security regulation targeting IoT users,[30] network strengthening, and active intervention[31] can successfully mitigate the harm of DDoS.

29. *Id.* at 1093–94. Cloudflare organized the persisting Mirai users into 33 independent C&C clusters, each with internally consistent naming patterns and exhibiting no shared data infrastructure with servers in other clusters. After Mirai's creators began working with the FBI, users of the Mirai botnet worked to outpace enforcement efforts. Cloudflare's monitoring schemata show that the software has spawned a number of progeny, each distinct from one the others. *Id; see also* Dan Goodin, *Assessing the Threat the Reaper Botnet Poses to the Internet—What We Know Now*, ARS TECHNICA (Oct. 27, 2017), https://arstechnica.com/information-technology/2017/10/assessing-the-threat-the-reaper-botnet-poses-to-the-internet-what-we-know-now [https://perma.cc/9W5X-JMGE]; Bradley Barth, *FYI, the OMG Mirai Botnet Variant Turns IoT Devices into Proxy Servers*, SC MAGAZINE (Feb. 22, 2018), https://www.scmagazine.com/home/security-news/iot/fyi-the-omg-mirai-botnet-variant-turns-iot-devices-into-proxy-servers/ [https://perma.cc/ZPM2-J3TW]; Zack Whittaker, *Fear the Reaper? Experts Reassess the Botnet's Size and Firepower*, ZDNET: ZERO DAY (Oct. 30, 2017), https://www.zdnet.com/article/reaper-botnet-experts-reassess-size-and-firepower/ [https://perma.cc/KY86-E44C]; John Leyden, *OMG, That's Downright Wicked: Botnet Authors Twist Corpse of Mirai into New Threats*, THE REGISTER (June 1, 2018), https://www.theregister.co.uk/2018/06/01/mirai_respun_in_new_botnets/ [https://perma.cc/DGY7-36WA]; David Holmes, *The Mirai Botnet is Attacking Again. . .*, DARK READING (Feb. 15, 2018), https://www.darkreading.com/partner-perspectives/f5/the-mirai-botnet-is-attacking-again/a/d-id/1331031 [https://perma.cc/V9VD-6T7A]. Mirai's targets before and after the creators' arrest had no unifying themes. They included popular target, Krebs on Security; Xbox, Sony, and Steam gaming platforms; Minecraft and Runescape servers; Chinese and Italian political dissidents' websites; and a Russian cooking blog. *See* sources cited and discussion *supra* note 14. More significantly, Mirai users attacked DNS servers belonging to Dyn, rendering nonoperational sites including Netflix, Amazon, Github, Reddit, Twitter, Paypal, HBO and others. *Id.*

30. Recently, California instituted regulations that would require that manufacturers of IoT devices to be sold in the state comply with informational security best practices, including robust passwords and automatic software updates. *See* discussion *infra* note 31.

31. One bottleneck on system penetration that approximates geography is nation-state law enforcement conducting regulatory or enforcement actions within their nation's boundaries. The F.B.I. and private U.S. corporations, for instance, actively work to manage botnets whose activities threaten both public and private interests within the nation. *See* discussion *infra* Section III.B. One basic method of doing so, however, is blackholing DNS servers, whereby an intervening actor identifies the path of communication between infected systems and the C&C server, then redirects traffic to a null location. *See* Anjali B. Kaimal, Aravind Unnikrishnan & Leena Vishnu Namboothiri, *Blackholing vs. Sinkholing: A*

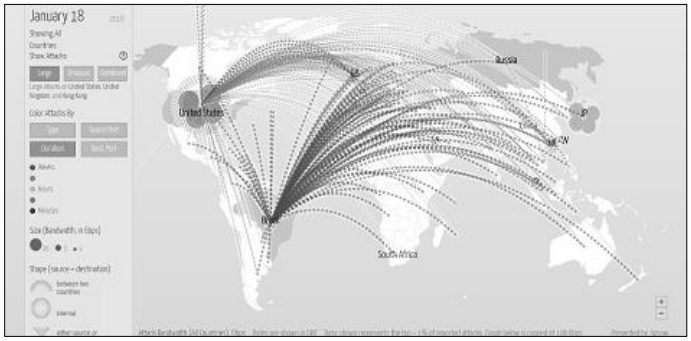
C. Where Are Botnets?

Traditional geography has little bearing on the establishment or use of a botnet. Defensive network security measures and offensive enforcement measures likely have greater bearing on where corrupted systems are located, and may cause infection rates to track with territorial boundaries.[32] Mirai infection, like that of many major botnets, is not significantly limited regionally,[33] and attacks do not originate from any one nation.

Comparative Analysis, 8 INT'L J. INNOVATIVE TECH. & EXPLORING ENG'G 15, 15–16 (2019). Various territories are likely to have differential incidence of botnet contribution as states impose information security regulations on both consumers and providers of IoT devices. *See, e.g.*, CAL. CIV. CODE § 1798.91.04 (West 2018) (requiring producers of internet-connected devices to comply with enumerated security requirements in order to sell to California consumers); *see also* Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, THE VERGE (Sept. 28, 2018), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law [https://perma.cc/8J9B-KS2R]; *but see* Robert Graham, *California's Bad IoT Law*, ERRATA SECURITY (Sept. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XEFd_VxKg2x [https://perma.cc/SME4-PKS5]. While the law has both cheerleaders and detractors, many are hopeful that this is the beginning of legislative interest in information security hygiene. *See generally* Derek Hawkins, *The Cybersecurity 202: California's Internet of Things Cybersecurity Bill Could Lay Groundwork for Federal Action*, WASH. POST: POWERPOST (Sept. 17, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.189dcc3fd688 [https://perma.cc/HB3Y-UTG8].

32. QUARTERLY THREAT LANDSCAPE REPORT, FORTINET 1, 17 (2018) ("The stark contrast among regions for the Andromeda botnet is rather shocking at first glance . . . [b]ut when you remember that it was the target of a major law enforcement takedown in late 2017, things come into perspective."); *see* Alan Charles Raul et al., *New York Enacts Stricter Data Cybersecurity Laws*, DATA MATTERS (Aug. 5, 2019), https://datamatters.sidley.com/new-york-enacts-stricter-data-cybersecurity-laws/ [https://perma.cc/XR8C-RK5F]; *see also* tbl.1 (demonstrating the relative infection rate of telnet devices in the case of the Mirai botnet). The data shows that certain nations have a higher prevalence of infection—in some cases, this phenomenon may be attributable to data security regulations.

33. *Compare* Antonakakis et al., *supra* note 6, at 1099 tbl.3 (showing the distribution of origins of infected systems participating in a 2016 DDoS attack on Krebs, a well-known internet security firm and perennial DDoS target) *with* FORTINET, *supra* note 32, at fig.11.



Consider a map illustrating DDoS activity in January 2018.[34] Each line between two nations represents contribution to the DDoS from devices in the originating nation. If more than 200,000 devices from dozens of sovereign nations contribute to an attack on servers located within the territory of a single sovereign nation, does the victim nation have a right to investigate the sources of that attack? Furthermore, to meaningfully intervene in a DDoS, enforcement must be able to track communications between a third-party C&C server and the device sending packets to the DDoS target. Often, to mitigate the damage caused by DDoS, responders must interfere with those communications.[35] Jurisdictional analysis, explained below, inquires whether units of data ("packets") sent from a DVR in Nation A to a C&C server in Nation B are so meaningfully extraterritorial that Nation C must persuade either the origin nation or the victim nation to provide legal assistance in a criminal investigation.[36] Strict adherence to limitations on extraterritorial enforcement action, explained below, would require an intervening cyber-capable nation to invoke negotiated information-sharing agreement with one or more nations

34. This map was made by Digital Attack Map, a resource showing live DDoS activity worldwide at www.digitalattackmap.com. Interacting with this map gives a clearer understanding of the frequency, magnitude, and scope of botnet activity. ©2018 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC. *See* Adarsh Verma, *This Live Map Shows Record-Breaking "Mirai" Malware Attacking your Country*, FOSSBYTES (Oct. 4, 2016), https://fossbytes.com/live-map-shows-record-breaking-mirai-malware-attacking-country/ [https://perma.cc/S7EJ-P4HQ].

35. Blackholing is a process by which a third party can nullify a botnet by locating the DNS server with the C&C server's IP address and remapping it to a dead-end location. *See* Kaimal et al., *supra* note 31.

36. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 221 (2d Cir. 2016) (describing the treaty-governed process by which sovereign nations share information regarding the production of extraterritorial evidence bearing on an ongoing criminal process).

through which the signals passed in order to monitor botnet activity.[37] This process, often pursued through mutual legal assistance treaties, is slow and deliberate. The President's Review Group on Intelligence and Communications Technologies reported that the average request took ten months to resolve.[38]

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act"), amending the Stored Communications Act to streamline evidence sharing. As a result, U.S. law enforcement now has the authority to compel disclosure of stored data by serving data storage companies with a warrant as described under the Act.[39] This regime will reduce the amount of time before responders receive required information, but the Act does not give access to all systems. The statute requires that responsive data belong to subscribers or users of service providers based in the United States. Moreover, the Act has drawn furor from privacy and human rights groups including the American Civil Liberties Union, the Electronic Frontier Foundation, Human Rights Watch, and Amnesty International.[40]

The CLOUD Act clears the path for U.S. law enforcement,

37. Congress passed the C.L.O.U.D. Act in 2018, requiring United States-based internet service providers to provide data at U.S. law enforcement's request regardless of where it is stored. 18 U.S.C. 2523 (2019) (amending the Stored Communications Act and giving it extraterritorial application); *see also* Kristin Houser, *Everything You Need to Know About the CLOUD Act*, FUTURISM (Mar. 26, 2018), https://futurism.com/everything-need-know-cloud-act [https://perma.cc/Y4H3-8F5E] (describing the deficiencies in the MLAT process as applied to cybercrime and how the CLOUD Act streamlines information sharing). While further discussion of the Act is outside the scope of this Note, Congress included in the amendments a provision authorizing bilateral information-sharing agreements, whereby party nations could serve data-holders directly so long as they require certain minimum procedural due process. *See* Press Release, U.S. Dep't of Justice, U.S. and U.K. Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), *available at* https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [https://perma.cc/2QFV-7R7K]; U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 4-6 (2019).

38. Richard A. Clark et al., THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD 171 (2014).

39. Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2703 (2019).

40. Aaron Mak, *Congress Put the CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy?*, SLATE (Mar. 22, 2018), https://slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html [https://perma.cc/Z7UE-53QL]; Russel Brandom & Colin Lecher, *House Passes Controversial Legislation Giving the US More Access to Overseas Data*, THE VERGE (Mar. 22, 2018), https://www.theverge.com/2018/3/22/17131004/cloud-act-congress-omnibus-passed-mlat [https://perma.cc/MK6K-MB9X].

but whether it incorporates international legal norms of privacy and territorial sovereignty is untested. Moreover, it does nothing to secure the internet as a whole; botnets beyond the reach of the CLOUD Act could still thrive without a broader grant of authority. Finally, an asymmetrical grant of authority in favor of the United States is unlikely to go unchallenged by adversaries or even peers. Bodies of multilateral treaty law and soft law are growing around these issues[41] and nations should assist them by encouraging global adoption of procedural norms and substantive law that anticipate rapid technical advancement and authorize capable nations to respond.

II. ANTI-BOTNET INTERVENTION

A. Early Anti-botnet Intervention: the Vigilantism Model

Some legal scholars have analogized, for normative purposes, the development of laws of cyberspace to those governing the sea, outer space, and to Antarctica—often to advance a particular theory of sovereignty in cyberspace.[42] Without addressing these analogies or normative approaches, this Note rather suggests, as a *descriptive* matter, that the trajectory of botnet mitigation in the United States has mirrored the development of law in the American frontier.

There, property rights were often enforced by private persons rather than by government, even into the twentieth century. Where law enforcement existed, it would sometimes draw from the private population—often those threatened by the criminal quarry at issue—to form posses.[43] Sometimes, permanent vigilante groups would develop either around communities or around industries, specializing in the types of criminal activity affecting the populations they served.[44]

41. Matthew Waxman, *International Law and Deterring Cyber-Attacks*, LAWFARE (Mar. 22, 2017), https://www.lawfareblog.com/international-law-and-deterring-cyber-attacks [https://perma.cc/8VFX-QURM] (discussing Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, INT'L SEC., Winter 2016/17, at 44); *see also* VIHUL ET AL., LEGAL IMPLICATIONS OF COUNTERING BOTNETS (2012), discussed *infra* Section III.C; discussion *infra* note 97 on the Budapest Convention.

42. Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69 (1998); Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A. F. L. REV. 1 (2009); *but see* Kristen Eichensehr, *The Cyber-Law of Nations*, 102 GEO. L.J. 317, 322 (2015).

43. W. C. Holden, *Law and Lawlessness on the Texas Frontier, 1875-1890*, 44 S. W. HIST. Q. 188, 198 (1940) (describing the quasi-lawful process of gathering a posse in order to deter crime in the American Southwest).

44. Paul Musgrave, *"A Primitive Method of Enforcing the Law": Vigilantism as a*

Similarly, in the absence of a clear governmental authority in cyberspace, private persons—including corporations—have taken the law into their own hands against botnets.[45] But like in the American West, optimal growth in cyberspace cannot be reached in a law enforcement vacuum, and the benefits of technological advances can redound more immediately to criminal actors than to law-abiding private persons. There, as here, "[c]ombating modern criminal organizations required a professional force that could only be funded and managed by . . . government."[46]

The evolution of counter-botnet intervention has followed a similar trajectory—from private actors vindicating their own rights to increasing governmental occupation of the field. Similarly, as law enforcement has endeavored to specialize, it has done so both through partnerships with the private sector and to the exclusion of private actors.

B. Private-Party Intervention

This Note is not the first publication to draw the analogy between cyberspace and the 'Wild West.'[47] The field, itself, has adopt-

Response to Bank Crimes in Indiana, 1925–1933, 102. IND. MAG. HIST. 187, 188–89 (2006) (describing the formation of vigilante groups by the Indiana Bankers Association in response to a rise in robberies during the period); Holden, *supra* note 43, at 198.

45. As discussed above, the barrier to interference with botnets is low, but targets are often incapable of protecting themselves with active measures. This Note discusses how private researchers and technology companies have interacted with botnets.

46. Explaining the move from private and vigilante systems to publicly funded law enforcement regimes, Musgrave writes:

> Technological and economic changes undoubtedly contributed to the new compact: it was far more difficult to train, equip, and coordinate thousands of vigilantes across an entire state than it had been for nineteenth-century citizens to organize against a handful of criminals. Combating modern criminal organizations required a professional force that could only be funded and managed by state government. And as the burden of ensuring order increased, so too did the incentives for individuals not to contribute to the provision of this public good; why, after all, should someone voluntarily pay for something that would otherwise have cost him nothing? (Such free-riding problems are major challenges for private law-enforcement mechanisms). [Eventually there developed] a new political reality in which, for practical purposes, the entire citizenry agreed that private agents' freedom to use violence for aims that they defined as public goods would henceforth be dramatically curtailed.

Musgrave, *supra* note 44, at 218.

47. *See, e.g.*, Matt Kimball, *IoT and Edge Computing: The Wild West of Cybersecurity*, FORBES (Nov. 20, 2018), https://www.forbes.com/sites/moorinsights/2018/11/20/iot-and-edge-computing-the-wild-west-of-cybersecurity/#1271cf7222d8 [https://perma.cc/FVE7-LMY3]; Claire Zaboeva, *The Wild West Era Has Ended — What's Next for Data Privacy?*, SECURITY INTELLIGENCE (July 16, 2019), https://securityintelligence.com/posts/the-wild-

ed the imagery of the Western film genre to organize its cast of characters. The 'bad guys,' those designing malicious code for criminal purposes, are known as "black hats" for the tell-tale accessory the villain would have worn in the movies. Across the street at high noon is the "white hat," the information security professional or penetration tester who uses his or her capabilities to advance security and prevent cybercrime, usually as a part of his or her employment. Watching from the window of the saloon is the unaffiliated "gray-hat" hacker, who hacks according to their individual moral code. The vulnerabilities he or she identifies may be disclosed, publicized, or even sold.[48]

In 2009, researchers at the University of California at Santa Barbara ("U.C.S.B.") took on the gray-hat role when they took over the Torpig botnet.[49] Botnets are subject to takeover or disruption by any private person who can interact with the C&C server, the DNS containing the C&C server's address, the infected devices, or the flow of traffic. In organizing and effecting the Torpig takeover, the U.C.S.B. team took on both governmental and outlaw traits. First, they established principles by which they would operate the botnet after acquiring control, focusing on harm minimization, security of stored data, and remediation.[50]

While the U.C.S.B. team was careful not to execute orders that might continue Torpig's criminal theft protocol, its members were aware that they could incur criminal liability, that they could be DDoSed—or killed, they feared—by the criminal actors, or that their systems could be taken down by the internet service provider.[51]

---

west-era-has-ended-whats-next-for-data-privacy/ [https://perma.cc/T36U-WF8Y]; Levi Gundert, *Taming the Digital Wild West*, DARK READING (Jan. 3, 2019), https://www.darkreading.com/threat-intelligence/taming-the-digital-wild-west/a/d-id/1333569 [https://perma.cc/WS26-Y75P].

48. This sale of vulnerabilities seems illicit, but both private industry and government agencies pay for zero-day vulnerabilities on the gray market. *See* Eichensehr, *supra* note 42.

49. Brett Stone-Gross et al., Your Botnet is My Botnet: Analysis of a Botnet Takeover 18 (Jan.–Feb. 2011) (working paper) (on file with author); GoogleTechTalks, *How to Steal a Botnet and What Can Happen When You Do*, YOUTUBE (Sept. 21, 2009), https://www.youtube.com/watch?v=2GdqoQJa6r4&t=1603s [https://perma.cc/X4YL-KFQJ] (explaining how the presenter, along with the rest of the U.C.S.B. team, monitored and acquired the botnet).

50. GoogleTechTalks, *supra* note 49, at 24:10. Consider how these tenets mirror the norms described by Professor Ashley Deeks and discussed *infra* at Section IV.B.

51. *Id*. at 52:45 ("I don't know who I was more afraid of—the criminals or law enforcement. . . . [W]e didn't get any permission to do this. We're cowboys from U.C.S.B. . . . [M]ore importantly, we don't want to notify someone who would just say 'shut it down.'"); *Id*. at 51:05 ("On January 25th . . . my biggest concern was the criminals—because these guys were known to be bad guys—were going to come and get us and shoot

Legally, the U.C.S.B. researchers had no more authority to exercise control over this botnet than the malicious actors did. The various tools and methods of researching botnets could bring researchers into conflict with the law. The use of tools that permit observers to see the content of communications as they travel (what this Note will call "content data") could violate the Wiretap Act.[52] Even monitoring the trajectory of communications including the communication's source, target, and route (what this Note will call "traffic data") could be a violation of the PATRIOT Act.[53]

During the ten days the researchers controlled the Torpig botnet, they downloaded nearly 70 gigabytes of data. They did not know what this data would be before they began the operation but quickly realized that it contained personal identifying information, bank account credentials, and credit card numbers.[54] This could bring their activities under the Computer Fraud and Abuse Act ("C.F.A.A."),[55] a near catch-all criminal statute that has been criticized for its broad applicability and generous jurisdictional hook.[56] In 2013, a gray-hat botnet researcher named Marcus Hutchins, also

off our kneecaps. . . . [M]ore realistically we were concerned they were going to DDoS us.").

52. 18 U.S.C. § 2511 (2012) (amended 2018); *see also* Paul Ohm, Douglas Sicker & Dick Grunwald, *Legal Issues Surrounding Monitoring During Network Research* (Oct. 24–26, 2007) (SIGCOMM Invited Paper), *available at* http://conferences.sigcomm.org/imc/2007/papers/imc152.pdf [https://perma.cc/G9TY-EZFA].

53. 18 U.S.C § 3121(a) (2012) (amended 2018). Another popular term for this traffic information is "metadata."

54. Stone-Gross et al., *supra* note 49, at 24.

55. 18 U.S.C. § 1030(a)(2)(A) (2012) (effective Nov. 16, 2018).

56. *See* Recent Case, United States v. Nosal (Nosal II), *828 F.3d 865 (9th Cir. 2016)*, 130 HARV. L. REV. 1265 (2017) (describing how the eponymous case, which held that using a friend's password satisfied the "without authorization" prong of the offense, threatens to criminalize an enormous amount of innocent activity). The statute also made up eleven of the thirteen charges in the government's indictment of Aaron Swartz, a Harvard research fellow who connected his personal computer to the Massachusetts Institute of Technology's university network in order to download over 4,000,000 papers in the JSTOR archives. He was facing up to $1,000,000 in fines and up to thirty-five to fifty years imprisonment at the time of his suicide. Jim Zirin, *Aaron Swartz' Suicide Forces Hard Questions About the Criminal Justice System*, FORBES OPINION (Mar. 29, 2013), https://www.forbes.com/sites/jameszirin/2013/03/29/aaron-swartz-suicide-forces-hard-questions-about-the-criminal-justice-system/#1e6cea13331d [https://perma.cc/H43C-L2RE] (describing some conflict between Senator Cornyn's estimate that Swartz faced thirty-five years and the author's estimate of fifty years); *see* Indictment, U.S. v. Swartz, No. 11-cr-10260-NMG (D. Mass. 2011), ECF No. 2 (outlining the charges against Swartz); James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM. (Aug. 16, 2013), https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/ [https://perma.cc/86EX-RGPP].

known as MalwareTech, intervened in an enormous ransomware attack known as WannaCry.[57] The attack affected major private sector organizations, denying them access to their networks unless they paid a ransom in bitcoin. Hutchins observed the attack and located what he believed to be a web address associated with the botnet's C&C. He purchased the domain and rerouted all traffic to the address, creating a "black hole" for the malicious signal.[58] This played a critical role in mitigating the WannaCry attack, but it also attracted the attention of F.B.I. investigators. Hutchins recently pleaded guilty to manufacture and distribution of a communications interception device, namely the Kronos botnet.[59] Critics argue that anti-wiretapping statutes, like those charged in the Hutchins case, could apply to even more good-faith actors than the CFAA.[60] Some in the industry fear that this will chill research going forward, especially given that many able hackers have a history of working both within and against the law (whose prohibitions are still difficult to predict).[61] Increasingly, private-party intervenors have sought governmental authorization, or

57. Lily Hay Newman, *How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack*, WIRED: SECURITY (May 13, 2017), https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/ [https://perma.cc/AMX4-K25G]. Consider similarities between Hutchins' involvement and the tradition of gray hat or black hat private law enforcement—from which the term is derived—in the American frontier. N.B. this Note cites work by another famous gray hat, Mudge, *infra* note 70. Before Mudge was a senior project manager at D.A.R.P.A., he worked with an elite hacker group known as L0pht Heavy Industries and famously testified before Congress about potential methods and effects of latent threats in cyberspace.

58. *Id.*

59. Plea Agreement at 3, U.S. v. Hutchins, No. 17-CR-124 (E.D. Wis. Apr. 19, 2019), ECF No. 124 (describing the elements of 18 U.S.C. § 2512 (1)(c)(i)); Andy Greenberg, *Hacker Who Stopped WannaCry Charged with Writing Banking Malware*, WIRED (Aug. 3, 2017), https://www.wired.com/story/wannacry-malwaretech-arrest [https://perma.cc/F8C3-ZW94].

60. Lily Hay Newman, *WannaCry Hero's New Legal Woes Spell Trouble for White Hat Hackers*, WIRED (June 8, 2018), https://www.wired.com/story/wannacry-hero-marcus-hutchins-new-legal-woes-white-hat-hackers/ [https://perma.cc/D3BE-METY] (quoting Professor Ahmed Ghappour as saying that, "[i]f you were to stretch it to include development of malware, wiretapping provisions potentially have a broader scope than the Computer Fraud and Abuse Act and could really do an end-run on security research. . . . But researchers have a legitimate cause for concern that they might be subject to a technicality in the law. Frankly, it's something that we should all be concerned about, because we rely on these people for our security.").

61. *Id.*; Reeves Wiedeman, *Gray Hat*, N.Y. MAG. (Feb. 19, 2018), http://nymag.com/intelligencer/2018/03/marcus-hutchins-hacker.html [https://perma.cc/M7LM-HXM6] ("Hutchins has been a model of public-private cooperation at a time when the government was having difficulty recruiting cybersecurity talent. . . . Some security researchers said they would stop sharing information with the government in protest.").

even partnership, before acting. This model has become more fruitful as sophisticated technology companies adopted it in their own defense.

Microsoft drove the development of a litigation response to botnets in February 2010 when it filed suit against operators of the Waledac botnet in federal court. Microsoft alleged violation of intellectual property under the Lanham Act and won a temporary restraining order against the botmasters, permitting the company to blackhole the C&C servers.[62] In a second case, Microsoft initiated a lawsuit in conjunction with the Financial Services-Information Sharing and Analysis Center alleging that botmasters of the ZeuS botnet in Pennsylvania and Illinois were violating Microsoft's intellectual property by sending fraudulent links purporting to be official Microsoft publications and were furthermore violating federal anti-racketeering law.[63] The court agreed and permitted Microsoft—under the supervision and authority of the U.S. Marshals—to seize the C&C servers housing the botnet infrastructure identified in the suit.[64]

The ZeuS botnet case teaches how government actors can delegate enforcement authority to private sector experts to reach a mutually desirable outcome. But litigated solutions are increasingly untenable, most importantly because the speed with which damage occurs increases as technology improves, while the adjudicative process remains necessarily deliberative.[65] Insofar as the legal process

62. Nick Wingfield & Ben Worthen, *Microsoft Battles Cyber Criminals*, WALL STREET J. (Feb. 26, 2010), https://www.wsj.com/articles/SB10001424052748704240004575086523786147014 [https://perma.cc/A2S4-YYUV]; Complaint at ¶¶ 34–39, Microsoft Corp. v. John Doe, No. 1:10-cv-00156 (E.D. Va. Feb. 22, 2010).

63. Order for Permanent Injunction, Microsoft Corp. v. John Doe, No. 12-cv-01335 (E.D.N.Y. Dec. 5, 2012); Jeffrey Meisner, *Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets*, MICROSOFT: OFFICIAL MICROSOFT BLOG (Mar. 25, 2012), https://blogs.microsoft.com/blog/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets/ [https://perma.cc/TBF5-83J2]; Kim Zetter, *Microsoft Seizes Zeus Servers in Anti-Botnet Rampage*, WIRED (Mar. 3, 2012), https://www.wired.com/2012/03/microsoft-botnet-takedown/ [https://perma.cc/KWU2-Y5R3].

64. *See* Zetter, *supra* note 63.

65. Alhomoud et al., *supra* note 3, at 62 ("[S]uch cross-industry actions are too expensive and complex to implement against all cybercriminals, who control as many as a quarter of the world's computers."). This number, published in 2013, is relatively small compared to the systems available to criminal actors with the advent of IoT devices—many of which have negligible native security provisions and poor user security practices, as explained above. *See also* Thu Pham, *A Behind the Scenes Look at Creating DARPA's Cyber Analytical Framework*, DUO SECURITY: TECH TALK (Oct. 28, 2014), https://duo.com/blog/duo-tech-talk-a-behind-the-scenes-look-at-creating-darpa-s-cyber-

legitimates an enforcement action, the increasing extraterritoriality of botnet activities threaten to render U.S. court exercise of jurisdiction questionable.

Eventually, the equities at stake have led to a public-private partnership model that is increasingly weighted toward government actions.[66] Vindication of a private right in court is inefficient in this context. Cash-strapped, private actors—small businesses, private persons, developing nations—do not necessarily have the resources to maintain costly suits in federal court. The incentives of private-sector solutions are misaligned at scale. As targets diversify into global and public concerns, private industry will feel fewer incentives to drive solutions. It may also have less legal authority to do so, especially when many of the applicable domestic laws could be used symmetrically against both black- and white-hat hackers.[67] Furthermore, recruiting industry partners who have come to expect to benefit from botnet management by industry peers without internalizing the cost of enforcement could prove difficult.[68]

Peiter Zatko, known by his hacker handle, "Mudge," led the famed hacker think tank, L0pht Heavy Industries in the nineties and coined the term, "gray hat." Mudge and representatives from L0pht testified before the Senate on issues of cybersecurity, including DDoS, in 1998.[69] He would later go on to lead new projects at the

analytic-framework [https://perma.cc/75AJ-JPJN] ("He also compared the lines of code per security software, and graphed them over time. From 1985 to 2010, he found that the lines of code were increasing in volume, with more than 10,000,000 lines of code being found in Unified Threat Management software. He then plotted the average lines of code of malware, which evened out to 125 lines of code, which stayed steady over the same time period. That means, despite continued and increased efforts/longer lines of code, we are still attempting to combat malware that hadn't changed that much."). These numbers go to demonstrating that costly and time-consuming litigation does not compete with botnet-enabled cybercrime at scale, where new malware comes at a very low cost despite the consistent increase in damage new attacks can do.

66. Private firms will always be a part of this dynamic. Competition for government research and development contracts has proven to be a valuable incentive driving innovation in security.

67. *See* discussion *supra* II.B; *see also* ANGELOS D. KEROMYTIS, DARPA INFO. INNOVATION OFFICE, HARNESSING AUTONOMY FOR COUNTERING CYBERADVERSARY SYSTEMS (HACCS) 5 (2017), https://www.darpa.mil/attachments/HACCS_PD_Slides_QA_Final.pdf [https://perma.cc/N29H-TMKS] (acknowledging that "[a]ctive defense cyber operations against individual botnet nodes are difficult . . . [r]isky and illegal for the private sector, with no reward structure").

68. Here, we see the same free-rider problem discussed in Musgrave, *supra* note 44.

69. Joe Grand, *Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)*, YOUTUBE (Mar. 14, 2011), https://www.youtube.com/watch?v=VVJldn_MmMY [https://perma.cc/QPA7-4377] (transcription available at https://www.spacerogue.

Defense Advanced Research Projects Agency ("D.A.R.P.A.") and Google. He argued that the incentive model in private cybersecurity did not drive private cybersecurity firms to cure the problem—"to put themselves out of a job."[70] A zero-threat environment—the optimal result for the public and, therefore, for governments—does not sell antivirus subscriptions and is better effected by fast-acting, adaptive, state-driven, or public-private solutions.

C. The H.A.C.C.S. Solution to the Botnet Threat

On August 3, 2017, the U.S. Department of Defense's research wing, D.A.R.P.A., announced the Harnessing Autonomy for Countering Cyber-adversary Systems ("H.A.C.C.S.") initiative.[71] Through the H.A.C.C.S. initiative, D.A.R.P.A. hopes to "develop safe, reliable, and effective capabilities for conducting Internet-scale counter-cyber operations to deny adversaries' use of neutral . . . systems and networks (e.g., botnets)."[72]

The H.A.C.C.S. directorship explains in its program announcement that it would follow four steps. At the outset, the program would locate botnet-conscripted networks. Next, it would fingerprint those networks in order to track their development. Third, the program intends to exploit known ("n-day") vulnerabilities in associated systems to insert autonomous narrow artificial intelligence[73]

net/wordpress/?p=602 [https://perma.cc/LHR4-NL8M]).

70. *Id.*; Duo Security, *A Behind the Scenes Look at Creating DARPA's Cyber Analytic Framework (Mudge) – Duo Tech Talk*, YOUTUBE at 59:30 (Oct. 27, 2014), https://www.youtube.com/watch?v=Czf24RXIAAw [https://perma.cc/Q3PN-E9FS] [hereinafter Mudge] (explaining that the subscription model employed by major antivirus companies falls apart if these companies actually neutralize threats at their source); Thu Pham, *Duo Tech Talk: A Behind the Scenes Look at Creating DARPA's Cyber Analytic Framework*, DUO: DUO BLOG (Oct. 28, 2014), https://duo.com/blog/duo-tech-talk-a-behind-the-scenes-look-at-creating-darpa-s-cyber-analytic-framework [https://perma.cc/722J-7PLT].

71. Defense Advanced Research Projects Agency, Broad Agency Announcement: Harnessing Autonomy for Countering Cyber-adversary Systems (Aug. 3, 2017), https://www.fbo.gov/index?s=opportunity&mode=form&id=e37dc8983aa4347361744a3cfbb43ec5&tab=core&_cview=0) [https://perma.cc/5QC2-9FXL].

72. KEROMYTIS, *supra* note 67, at Slide 3.

73. N-day vulnerabilities are known software vulnerabilities (as distinct from vulnerabilities that have not yet been disclosed). Known vulnerabilities in popular consumer electronics or software are useful for both offenders and responders. They permit the former to deploy infectious malware and they permit the latter to install remedial code, sometimes called "white worms." Narrow artificial intelligence is machine learning that is designed to perform a particular function rather than a spectrum of functions.

("A.I.") "agents" into the infected network. These A.I. agents, as the director calls them, would act autonomously to diagnose and remediate the infection and ultimately neutralize malicious software at scale without disrupting the function of non-malicious or neutral systems.[74] The H.A.C.C.S. initiative is a useful technology to consider in the legal environment described in this Note. The directorship has organized its function into useful components. By following the methodological outline in the program announcement, this Note can consider how each function of the government's approach to botnets mitigation may interact with international law. Furthermore, the proposal incorporates emergent machine learning approaches to fingerprinting botnet traffic at scale, prompting interesting questions about the program's legal implications. The structure and the substance of the proposal suit the aims of this Note. Many of the program's moving pieces are analogous to previous botnet solutions. Finally, the H.A.C.C.S. announcement offers interested parties a peek at the strategic approach the United States is taking in botnet mitigation at scale. So even if H.A.C.C.S. as proposed does not become the dominant management technology, an analysis of its legal implications has value.[75]

The first step of the H.A.C.C.S. program—locating botnet-conscripted networks—involves machine learning algorithms trained to scan internet traffic for potential botnet signatures. Machine learning—a subset of artificial intelligence—is particularly suited to pattern recognition and outlier detection.

Consider diagnosis in oncology as analogous to fingerprinting a botnet. Put simply, cancer diagnosis is fundamentally a matter of recognizing normal tissue patterns in order to identify aberrant growth. In 2018, researchers in Germany, France, and the United States compared a deep learning algorithm's diagnostic performance against "a large international group of fifty-eight dermatologists from seventeen countries, including thirty experts with more than five years of dermoscopic experience."[76] When shown a 300-image test-

74. *See* KEROMYTIS, *supra* note 67.

75. Any mention of methodology with regard to either the D.A.R.P.A. program's proposal, the legal implications, or the potential remedies is largely based on a number of reasonable assumptions based on extant technologies. The choice to analyze the H.A.C.C.S. program in particular issues from its utility as a stand-in for current trends in botnet intervention as much as its own unique merits or its likelihood of being deployed as advertised.

76. H. A. Haenssle et al., *Man Against Machine: Diagnostic Performance of a Deep Learning Convolutional Neural Network for Dermoscopic Melanoma Recognition in Comparison to 58 Dermatologists*, 29 ANN. ONCOL. 1836, 1839 (2018). A convolutional neural network ("C.N.N.") is a type of deep learning algorithm that is particularly adept at

set, the deep learning algorithm decisively outperformed the human doctors on average and, in all but seventeen cases, individually.[77]

Machine learning in botnet tracking functions similarly. Because of the astronomical amount of data that goes into mapping the landscape of internet communications and because each botnet functions with some variance, machine learning is particularly well suited to the task of fingerprinting.[78] Furthermore, because machine learning algorithms teach themselves, under some degree of supervision, they resist obsolescence; they are well suited to countering a botnet's evasive techniques in a dynamic environment and over a span of time.[79]

The second function of the H.A.C.C.S. system is fingerprinting specific botnets. Different botnets incorporate different signatures—some overt and some merely discernable by monitoring idiosyncratic botnet behaviors in the wild.[80] To track the trajectory of botnets and detect vulnerabilities, responses to botnets at scale must incorporate data capture and storage, implicating privacy concerns.[81]

analyzing visual data, but practitioners have shown how such a tool can be augmented with other machine learning techniques to handle packet-transfer traffic data. *See* Rimmer, *infra* note 79.

77. Haenssle, *supra* note 76, at 1839 ("When dermatologists were provided with dermoscopic images only (study level-I) their dichotomous classification of lesions was significantly outperformed by the C.N.N. However, in a real-life clinical setting, dermatologists will incorporate more clinical information into decision-making. Therefore, we investigated the effect of additional clinical information and close-up images and found a much-improved diagnostic performance of dermatologists (study level-II). However, at their improved mean sensitivity (88.9%) dermatologists still showed a specificity inferior to the C.N.N. (75.7% versus 82.5%, P<0.01).").

78. Hoang & Nguyen, *supra* note 11.

79. *Id.*; NDSS Symposium, *NDSS 2018 – Automated Website Fingerprinting through Deep Learning*, YOUTUBE at 05:45 (Mar. 14, 2018), https://www.youtube.com/watch?v=fxYUVVq0T1g [https://perma.cc/GQ5Y-L9L9] (explaining that deep learning automatically discovers features from raw data, obviating hand engineering and allowing the algorithm to adjust automatically when traffic data changes). In this way, deep learning algorithms are well suited to responding to evasive maneuvers built into botnet malware. *See* Vera Rimmer et al., *Automated Website Fingerprinting through Deep Learning*, NETWORK AND DISTRIBUTED SYSTEMS SECURITY (NDSS) SYMPOSIUM (2018); Yu et al., *supra* note 10 (discussing domain flux).

80. *See generally* Boukhtouta et al., *supra* note 10 (describing the process by which their team built its malware-fingerprinting algorithm). N.B. the report details that their algorithm actually requires traffic—rather than content—data in order to sidestep encryption. This element of botnet interdiction becomes relevant in the discussion of substantive privacy issues at III.B. *See also* discussion *infra* Section III.C.

81. *Id.* at 551 ("The network traces parser is integrated to pick up values for different attributes (features) from network packets. All resulted values are stored in feature files that

This Note will discuss the international privacy concerns that vast arrays of stored communications metadata are likely to provoke.

Third, efficaciously dismantling a botnet network implicates some degree of interference with the function of neutral computer networks.[82] This begins with interrupting malicious signals sent between systems, but ultimately—in order to disrupt a botnet for a meaningful period—there must be some persistent remedial device.[83] This period of remission allows responders to patch vulnerabilities and adapt antiviral software to the peculiarities of the malicious code.

This final element of the H.A.C.C.S solution—neutralizing malicious code on conscripted networks—will likely involve the highest degree of interference with systems. In order to render a permanent solution, responders may need to alter stored data (including the infectious code). This could potentially cause damage to neutral systems, which could rise to the level of a violation of a host nation's law. Until international law develops instruments authorizing cyber-capable states to engage in such interference, these solutions will likely be limited to extant methods of remediation—patching vulnerabilities and chasing new malware as it develops.

III. HOW DOES THE LAW LIMIT OR ANIMATE EXPANDING ENFORCEMENT ACTIVITY?

A. Enforcement Jurisdiction in International Law

Jurisdiction is a threshold requirement for transnational enforcement action by nations. There are two axes to jurisdiction: what a state may do and to whom a state may do it. Regarding what

are readable with data mining artifacts." N.B. the high level of abstraction at which the data is stored after being reviewed by the algorithm. This becomes relevant when considering substantive privacy concerns examined at III.B). *See also* discussion *infra* Section III.C.

82. VIHUL ET AL., *supra* note 41, at 38–41 (describing how interference with a botnet could constitute interference with data or computer systems under European law); *compare* Section III.B, describing how this interference can but should not be considered interference under similar provisions of international law. *See also* discussion *infra* Section III.C.

83. *Compare* VIHUL ET AL., *supra* note 41, at 45–46 (describing use of a 'white worm'), *with* KEROMYTIS, *supra* note 67, at Slide 6 (describing "autonomous [A.I.] agents that can be introduced into gray networks at scale to counter botnets and similar adversarial implants"); *see also* KEROMYTIS, *supra* note 67, at Slide 41 (explaining that "[p]ersistence [of agents] may be part of the rules of operation [but that] persistence is to be a limited time duration." N.B. this persistent agent model of remedy may be less offensive to law than a remedy that relies on state actors deleting or altering software (i.e., malware) on host computers without permission from the host).

a state may do, international law recognizes three types of jurisdiction: prescriptive, adjudicative, and enforcement.[84] This Note deals with enforcement jurisdiction implications of various anti-botnet measures taken by victim nations. It describes the measures already taken by some countries and how the unique complications of this breed of digital crime could limit a responding nation's assertion of jurisdiction over an anonymized foreign offender.[85]

On over whom a state can exercise jurisdiction, customary international law is simple: (a) a state may exercise jurisdiction to enforce in its own territory, and (b) a state may not exercise jurisdiction to enforce in the territory of another state without . . . consent."[86] This default rule—that enforcement jurisdiction is coextensive and coterminous with a nation's territorial boundaries—is usually traced to the Peace of Westphalia, seventeenth-century Europe's conclusion that a negotiated legal order and balance of power was an existential necessity for life on the continent.[87] But globalization has required

84. Restatement (Fourth) of Foreign Relations Law of the United States § 401 (Am. Law Inst. 2018) [hereinafter Restatement].

85. Prescriptive jurisdiction deals with a state's power to prescribe and regulate activity over persons. *See id.* This Note does not touch on this aspect of jurisdiction except to note the Budapest Convention's attempt to harmonize the domestic criminal laws of acceding states to make enforcement authority clearer. Adjudicative jurisdiction deals with the power of a state's courts to apply that state's laws to a person within its enforcement jurisdiction. *See id.* This Note will not deal with adjudicative jurisdiction because targets of enforcement, in this context, are unlikely to claim a violation of jurisdiction in a victim nation's courts.

86. Restatement, *supra* note 84, § 432.

87. *See* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 556–57 (1987) (Blackmun, J., concurring in part and dissenting in part) ("Under the classic view of territorial sovereignty, each state has a monopoly on the exercise of governmental power within its borders and no state may perform an act in the territory of a foreign state without consent."); STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 20 (1999) ("The fundamental norm of Westphalian sovereignty is that states exist in specific territories, within which domestic political authorities are the sole arbiters of legitimate behavior."); Daud Hassan, *The Rise of the Territorial State and the Treaty of Westphalia*, 9 Y.B. N.Z. JURIS. 62, 64 (2006); Jean-Baptiste Maillart, *The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime*, 19 ERA F. 375, 375–76 (2019) ("[I]t is indeed indisputable that the generally accepted view in public international law is that the primary basis of criminal jurisdiction for any state is territorial. This is to be explained mostly by the existence of very strong ties between the notions of state sovereignty ad territoriality, the latter being the necessary corollary of the former in the Westphalian legal order." (quotations and citation omitted)); Michael Chertoff, *The Responsibility to Contain: Protecting Sovereignty Under International Law*, FOREIGN AFF., Jan.–Feb. 2009, at 130, 132 ("Under the Westphalian model of sovereignty—which dates back to 1648—an independent state is not subject to external control over its internal affairs without its consent.").

the expansion of enforcement authority by states.[88]

The Lotus Case was an early example of legal conflict over enforcement jurisdiction where territoriality confused, rather than determined, whose authority predominated.[89] The case remains customary international law's touchstone for the exercise of criminal enforcement jurisdiction in the event of an extraterritorial or transnational harm.[90] There, French and Turkish vessels collided in international waters, killing eight sailors and sinking the Turkish vessel. After the French ship, the *S.S. Lotus*, brought the survivors to the Turkish port, Turkey arrested, convicted, and sentenced the *Lotus's* first officer and captain to 80 days imprisonment and a fine. France sued Turkey in the League of Nations' Permanent Court of International Justice ("P.C.I.J."), claiming that Turkey violated international law by exercising jurisdiction over French sailors and requested that Turkey be ordered to release the French sailors into French custody. The P.C.I.J. disagreed.

The dual principles at issue in *The Lotus Case* can be stated as follows. First, nations may not exercise extraterritorial enforcement jurisdiction "except by virtue of a permissive rule derived from international custom or from a convention."[91] Second, absent restrictions to which any state—in its own discretion—may bind itself, a state may presumptively exercise enforcement jurisdiction over actors within its own territorial boundaries as an aspect of its sovereignty.[92]

Applying these principles, the *Lotus* court concluded that both nations had concurrent jurisdiction over the actors involved in the incident at sea and that Turkey did not violate international law by exercising that jurisdiction over French sailors within its territorial boundaries.[93]

Botnet-enabled cybercrime and the question of data territoriality test intuitive notions of the presumptive territorial jurisdiction

88. *See* LOUIS HENKIN, INTERNATIONAL LAW: POLITICS, VALUES AND FUNCTIONS 313 (1990) ("Increasingly, the international system has recognized that the concept of enforcement is broader than commonly assumed. . . ."); *but see id.* at 315 ("Increasingly, States in whose territory these activities take place, or whose nationals or companies are affected by such administrative enforcement, have invoked international norms to challenge excesses or inadequacies.").

89. S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

90. *The Lotus Case* is often cited for the proposition that that which is not outlawed is permitted in international law. But the narrower holding of the case—that of determining the choice of enforcement jurisdiction in the case—bears directly on the issue in this Note.

91. S.S. Lotus, 1927 P.C.I.J. (ser. A) No. 10, ¶ 45.

92. *See id.* ¶¶ 46–47.

93. *Id.* ¶ 87.

described by the *Lotus* court. While nations may criminalize transnational or foreign acts that cause harm within their own boundaries,[94] the *Lotus Case* teaches that without a positive source of international law, State A's enforcement actions against the criminal actor inside the territorial boundaries of State B are disallowed.[95]

International law has repeatedly and recently affirmed the notion that state-controlled botnet-enabled crime and the failure to act against perpetrators of denial of service attacks violate both treaty and customary law.[96] Absent law that empowers nations to act against extraterritorial threats, and in light of the transnational nature of botnets, nations must either act outside of the law—or against it—or they must simply hope that nations hosting criminal actors intervene. But by harmonizing criminal law against botnets and approaching recognition of an affirmative duty to act, discussed below, the community of nations is moving toward a body of law that understands the universal threat of botnets and the currently asymmetric capabilities of intervening nations.[97]

94. International law calls this effects-based jurisdiction. *See* Restatement, *supra* note 84, § 409.

95. This is the traditional presumption stated simply, and it is in the shadow of this presumption that states negotiate mutual assistance treaties and establish new norms of conduct in cyberspace.

96. *See, e.g.*, COUNCIL OF EUR., CYBERCRIME CONVENTION COMM., T-CY GUIDANCE NOTE #2: PROVISIONS OF THE BUDAPEST CONVENTION COVERING BOTNETS (2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 [https://perma.cc/M6W4-9VR8] (mapping the elements of botnets onto provisions of criminal law adopted by signatory nations); COUNCIL OF EUR., CYBERCRIME CONVENTION COMM., T-CY GUIDANCE NOTE #5: DDOS ATTACKS (2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e9c49 [https://perma.cc/TPT2-AQ35] (mapping the elements of botnet-enabled crime onto provisions of criminal law adopted by signatory nations). *See* discussion *infra* Section IV.B.

97. *See* discussion *infra* Section IV.B. Furthermore, the Budapest Convention on Cybercrime, discussed *infra*, is considering provisions dealing with establishment of such a duty and jurisdiction-sharing mechanism. *See* COUNCIL OF EUR., CYBERCRIME CONVENTION COMM., CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY ¶ 47 (2016) ("The location of the victim at the time of the crime in the territory of a Party may also support a claim for jurisdiction and if needed (unilateral) transborder access to data, within agreed upon limitations."); Chertoff, *supra* note 87, at 131–32 (speaking normatively about an international legal order centered around "a new principle, under which individual states assume reciprocal obligations to contain transnational threats emerging from within their borders so as to prevent them from infringing on the peace and safety of fellow states around the world."); Dan E. Stigall, *Counterterrorism, Ungoverned Spaces, and the Role of International Law*, SAIS REV. INT'L AFF., Winter–Spring 2016, at 47, 51 ("The most obvious means by which international law can facilitate counterterrorism efforts in ungoverned

B. Early Legal Analysis of Botnet Mitigation: Substantive Domestic Law

Early analysis of anti-botnet enforcement naturally focused on domestic action. But as botnets have become larger and more overtly transnational in scope and effect, it is less clear that a domestic-law framework is a useful starting point for botnet mitigation.

In 2012, the North American Treaty Organization ("N.A.T.O.") Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency ("E.N.I.S.A.") published a report that illuminates some of the ways in which competing legal regimes could complicate the study of botnets as well as efforts to manage them. In the report, The Legal Implications of Countering Botnets, the authors outlined how researchers and responders may interact with various European criminal and civil laws governing data privacy and surveillance.[98]

The report—using Estonian and German law as stand-ins for European law—examines how each of five discrete steps involved in typical enforcement operations can run afoul of the law[99] and attempts to harmonize necessary technological interference with regulations. It also imagines a scenario where remediation of malware-infected systems could do harm to private property in violation of the host nation's laws.[100] But the trend toward increasing transnationality of these networks, explained above,[101] complicates the legal implications even further than the authors anticipate.

The report's abstract reads: "The implementation of [botnet-reduction] methods needs to take place according to the legal systems

spaces is through its enabling functions that permit outside actors (capable states and/or, in certain circumstances, international organizations) to intervene and perform functions fragile states cannot."). Stigall's recommendations mirror Chertoff's. In his article on counterterrorism in ungoverned spaces, Stigall suggests that an international legal order that prioritizes a sovereign's duty to act against destabilizing acts within its boundaries, and a concomitant power in other nations to intervene in response to a failure to contain a transborder harm, will increase global security, especially when accompanied by increased information sharing. This Note discusses how these principles should drive international legal developments in cybersecurity.

98. *See* VIHUL ET AL., *supra* note 41.

99. *Id.*

100. *Id.* at 46 ("The use of white worms constitutes an interference with data processing operations as well, as the worm wipes out or at least manipulates the infected data. This might damage . . . programs or essential functions. . . . Since such potential collateral damage is not endorsed, the automated disinfection method is a criminal act.").

101. *See* discussion *supra* Section I.C.

of the respective jurisdictions."[102] But mapping subjective and objective jurisdiction onto the kaleidoscopic territorial implications of botnet-driven crime complicates the jurisdictional question beyond simple application of the *Lotus* principles. As an intuitive exercise, whose jurisdiction should predominate over digital packets sent from an Estonian computer system without a user's knowledge by an autonomous malware maliciously installed—again autonomously—in a sequence of millions of iterations of autonomous code in a chain of several thousand systems in dozens of sovereign territories originating from a remote criminal's system whose home jurisdiction is hidden by data-anonymizing software?[103] Do European and Estonian authorities have exclusive authority to govern a remedy to this system's contribution within a network of millions of infected systems?[104] Are these packets, the contents of which are not relevant to the attack, a communication for the purpose of privacy law?[105]

Who are the parties to this communication under the law? And within which jurisdiction is it observed when the university researcher or the F.B.I. Special Agent observes the traffic data of these packets in light of the fact that digital communications typically travel across many territorial boundaries, often in unpredictable or counterintuitive paths?[106]

None of these questions can be answered neatly. Meanwhile, the report concedes that the probability that a host initiates suit against a researcher acting in good faith is uncertain, as is that of a botmaster bringing suit claiming violation of a privacy or proprietary interest.[107] The logic of wielding domestic law as an effective response to transnational cybercrime breaks down here. In many of the

102. VIHUL ET AL., *supra* note 41, at 1.

103. N.B. that the question of whose jurisdiction predominates is not a necessary question in transnational criminal adjudication or enforcement. But this Note questions whether the law follows intuition in the application of old laws to new technology.

104. *See* Kim Zetter, *Bredolab Bot Herder Gets 4 Years for 30 Million Infections*, WIRED (May 23, 2012), https://www.wired.com/2012/05/bredolab-botmaster-sentenced/ [https://perma.cc/GU59-EXZG]. It is not uncommon for botnets to infect millions of systems, though botnets such as Mirai with a more limited breadth may pose a disproportionately high threat. However, when considering the practicability of interfering with host systems, practitioners should consider the maximum scope of infection.

105. *See* discussion *infra* Section III.C.

106. *See* Christopher Groskopf & Sarah Slobin, *Where Your Data Flows on the Internet Matters, and You Have No Control Over It*, QUARTZ: MAP OF THE INTERNET (Oct. 5, 2016), https://qz.com/741166/where-your-data-flows-on-the-internet-matters-and-you-have-no-control-over-it/ [https://perma.cc/K3ZF-6EYS].

107. *See* VIHUL ET AL., *supra* note 41.

scenarios considered, the report suggests that good-faith researchers of botnets may incur liability that approaches symmetry with that of bad-faith botnet controllers.[108] The incentive structure of such a legal outcome is inverted. Here, deterrence is felt first by the innocent researcher, the private sector security partner, and the transnational law enforcement agent, each of whom operates more openly than their malicious opponent. By chilling these actors, the bad-faith and well-anonymized criminal moves with alacrity and relative impunity[109] throughout systems in nations that do not enjoy robust network security and anti-botnet enforcement tools.

Governance by many domestic criminal regimes, each potentially in conflict with the other, can make cyberspace difficult to navigate for actors operating in good faith. White- and gray-hat hackers may not know, at any point, who operates the systems they interact with or where they are located. Fears that they may violate a hostile nation's criminal laws are legitimate, and without multinational agreements harmonizing the rules by which they operate, reasonable actors are likely to err on the side of caution, leaving potential discoveries behind.

C. How Could International Law Constrain Anti-Botnet Enforcement?

Since 2013's revelations about U.S. mass monitoring of transnational communications, groups have sought to apply extant human rights and privacy law to surveillance. Application of pre-cyber international law has not lit the path for either law enforcement or privacy advocates much better than the patchwork of domestic criminal regimes, but some trends are emerging.

The primary legal constraints on anti-botnet measures at scale, if any, will likely issue from laws governing surveillance and by extension, privacy and human rights. In this section, the Note will introduce the United Nations' International Convention on Civil and Political Rights ("I.C.C.P.R."), a leading source of international privacy law, describe the controversy surrounding its application to foreign surveillance, and consider possible interpretations of its provisions where it applies to large-scale botnet management programs. And while large-scale botnet-management programs may not engage in surveillance within the meaning of these sources of law, this Note

108. *See generally id.*

109. Eoyang et al., *supra* note 18, at 1, 3 (estimating that only 0.3% of reported cybercrime incidents result in an arrest).

will largely assume that these laws will apply for the purposes of its discussion.

After 2013's revelations about the N.S.A.'s bulk metadata storage program and American surveillance of allied leaders, members of the international legal community—led by Germany and Brazil—made a push to establish stricter international regulations on transnational surveillance.[110] Eventually, the U.N. Human Rights Council took up the issue.[111]

During this time, the official position of the United States was that the I.C.C.P.R. only covered persons within its geographical confines.[112] For years, scholars and nations struggled with the question of extraterritorial applicability. In his article, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age," Marko Milanovic, then Secretary-General of the European Society of International Law concedes that whether the provision has extraterritorial effect is unclear, perhaps even unlikely, despite the fact that he believes that the law *should* control.[113]

Grappling with this and other questions surrounding surveillance and international law, the U.N. General Assembly Third Committee published its resolution, "The Right to Privacy in the Digital Age."[114] Despite the animus with which the effort began, the conclusions of the committee were such that the United States approved of the report and its conclusion that "the same rights that people have

110. Colum Lynch, Shane Harris & John Hudson, *Exclusive: Germany, Brazil Turn to U.N. to Restrain American Spies*, FOREIGN POL'Y: THE CABLE (Oct. 24, 2013, 8:18 PM), https://foreignpolicy.com/2013/10/24/exclusive-germany-brazil-turn-to-u-n-to-restrain-american-spies [https://perma.cc/8Y3U-D74H]; *accord* Colum Lynch, John Hudson & Shane Harris, *Exclusive: Twenty-One Nations Line Up Behind U.N. Effort to Restrain N.S.A.*, FOREIGN POL'Y: THE CABLE (Oct. 25, 2013 6:50 PM), https://foreignpolicy.com/2013/10/25/exclusive-21-nations-line-up-behind-u-n-effort-to-restrain-nsa [https://perma.cc/GR4P-9NJN]; *accord* Colum Lynch, *Exclusive: Inside America's Plan to Kill Online Privacy Rights Everywhere*, FOREIGN POL'Y: THE CABLE (Nov. 20, 2013, 6:10 PM), https://foreignpolicy.com/2013/11/20/exclusive-inside-americas-plan-to-kill-online-privacy-rights-everywhere [https://perma.cc/UDD3-KNDX]; *accord* Colum Lynch & Ty McCormick, *Dilma Blasts U.S. Spies as International Crooks*, FOREIGN POL'Y: THE CABLE (Sep. 24, 2013, 1:00 PM), https://foreignpolicy.com/2013/09/24/dilma-blasts-u-s-spies-as-international-crooks [https://perma.cc/H2T2-ATN4].

111. *See* Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014).

112. Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 307 n.49 (2015).

113. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 111 (2015).

114. G.A. Res. 69/166 (Feb. 10, 2015).

offline must also be protected online, including the right to privacy" as embodied in article seventeen of the I.C.C.P.R.[115]

In the U.N. Human Rights Committee's 2014 Concluding Observations on the Fourth Periodic Report of the United States of America (the "H.R.C. Report"), the United Nations first made clear that it interpreted the jurisdictional provision of the I.C.C.P.R. to cover extraterritorial surveillance.[116] Moreover, it expressed frustration at the N.S.A.'s bulk metadata collection program.[117] It went on to admonish the government to:

> Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of [(a)] legality, [(b)] proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.[118]

The first structure—the principle of legality—requires that the act taken is in accordance with the state's domestic law.[119] This principle requires that the act taken is in accordance with the state's domestic law. When the Senate Committee on Foreign Relations issued its report pursuant to ratification and signing of the I.C.C.P.R., the only understanding expressed applying to article seventeen of the document was that they understood the document to be non-self-executing.[120] This was "to clarify that the Covenant will not create a private cause of action in U.S. courts" and that as "existing U.S. law generally complies with the Covenant . . . implementing legislation is not contemplated."[121] If a state must authorize a new enforcement mechanism through legislation, however, that act must also comply with the treaty. The U.N. Report on the Right to Privacy contem-

115. *See id*. at 3.

116. U.N. Human Rights Comm., Concluding Observations on the Fourth Periodic Report of the United States, U.N. Doc. CCPR/C/USA/CO/4, at 2 (Apr. 23, 2014).

117. *Id.* at 10.

118. *Id.* at 11.

119. *See* Press Release, U.S. Office of the Press Sec'y, Presidential Policy Directive—-Signals Intelligence Activities § 1(a) (Jan. 17, 2014) ("The collection of signals intelligence shall be authorized by statute or Executive Order" and must be undertaken in accordance with U.S. law.).

120. S. EXEC. DOC. No. 102–23, at 9, 19 (1992).

121. *Id.*

plates a situation where, in order for interference to pass legal muster, a nation may have to pass accompanying legislation giving the public proper notice of the scope of the interference.[122]

Article seventeen also requires that interference be non-arbitrary (i.e., proportional and necessary). David Kaye, writing as amicus for Appellant in *Doe (Kidane) v. Federal Democratic Republic of Ethiopia* interpreted this requirement in the following way: "A number of international bodies and experts – including the Human Rights Committee, the U.N. High Commissioner for Human Rights, and various U.N. Special Rapporteurs—conclude that an interference with privacy is non-arbitrary only if it is necessary to achieve a legitimate aim, proportionate to the aim sought."[123] This language approximates the application of similar provisions of the European Commission on Human Rights.[124] In applying these provisions in *Weber and Saravia v. Germany*, the European Court of Human Rights ("E.Ct.H.R.") ruled that while Germany had clearly interfered with applicants' privacy, the reasonableness of the interference was proportional to the weighty national security interests at issue.[125]

122. Rep. of the Office of the U.N. High Comm'r for Human Rights, *supra* note 111.

123. Brief for John Doe, a.k.a. Kidane, as Amici Curiae Supporting Plaintiff-Appellant at 13–14, 16–17, Doe v. Ethiopia, 851 F.3d 7 (D.C. Cir. Nov. 23, 2016), (No. 16-7081).

124. *See* European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S. No. 5, 213 U.N.T.S. 221 ("1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."). *See also* Milanovic, *supra* note 113, at 101–102 (comparing the I.C.C.P.R. and the E.C.H.R.). N.B. that beyond this Note's analysis of whether pre-cyber human rights law does any useful work in signals monitoring, the propriety of application of these principles to online communications is not universally approved. *Id.* at 110 ("Instead of looking at the object and purpose of the ICCPR at a general level one could also inquire into the intentions of the parties as to the specific problem of extraterritorial application [of the ICCPR]. Put aside for a moment the fact that we are actually unable to determine this with much confidence from . . . the methodological dubiousness of assuming what the text's drafters would have wanted if they were to decide a particular hypothetical. I am happy to concede that if we could today resurrect the drafters of the ICCPR and the ECHR, educate them about emails, the Internet, and smartphones, and ask them whether their treaties should apply to overseas espionage and mass surveillance programs of the kind run by the NSA and GCHQ, their answer would likely be no."). Here, Milanovic sounds more like Chertoff, discussed *infra*, in calling for interpretation of these provisions on a model of sovereign consent—instead of analogizing signals surveillance and human rights, asking whether nations have agreed to be bound to such barriers, and to what extent.

125. Weber and Saravia v. Germany, 2006-XI Eur. Ct. H.R. 1173.

Consider yet another possible meaning for proportionality: David Kaye, as special rapporteur, wrote that "[a] proportionality assessment should ensure that the restriction is 'the least intrusive instrument amongst those which might achieve the desired result.'"[126] Here, again, the notion of minimization of intrusion legitimates governmental interference in the pursuit of a legitimate aim.

When considering the trajectory of application of privacy law to foreign surveillance, some look to the E.Ct.H.R. for guidance.[127] The court, applying a similar provision in Article Eight of the European Convention on Human Rights ("E.C.H.R."), recently gave a broad grant of jurisdictional authority to the E.C.H.R.'s privacy provision in *Big Brother Watch and Others v. United Kingdom*.[128] Considering a regime whereby British intelligence services had directed N.S.A. to intercept communications of foreign nationals as part of an intelligence-sharing regime connected to N.S.A.'s bulk metadata collection program, the E.Ct.H.R. voiced Article Eight's test for the propriety of bulk surveillance.[129] The nine-element conjunctive standard for the "compatible with the rule of law" test (i.e., the prin-

126. U.N. Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, ¶ 35 U.N. Doc. A/HRC/29/32 (May 22, 2013) (citing International Covenant on Human Rights art. 40, ¶ 4 cmt. 27, Nov. 1, 1999, 99 U.N.T.S. 171). *See* Boukhtouta, *supra* note 10, at 549 (describing how preliminary studies involved labeling of certain content as malign and other as benign, but the eventual failure to track and fingerprint this data at scale and when encrypted. In order to sidestep this shortcoming, the team instead employed a traffic-data analytic tool that would fingerprint malignant data from the point of view of an internet provider. "The packet content approach . . . fails in capturing badness when the traffic is encrypted. Moreover, it needs sampling to preserve scalable detection at the presence of a large traffic. Our approach is a malware network behavioral based rather than content based to avoid these two limitations."); *see* Uzun v. Germany, App. No. 35623/05, Eur. Ct. H.R. (2010) (holding that GPS location data was less intrusive than visual or acoustic data providing the same location information because it gave up less information about the target's personal thoughts or opinions); *compare* Convention on Cybercrime, art. III.2.33, Nov. 23, 2001, ETS No. 185 [hereinafter Budapest Convention], *with* Budapest Convention, art. III.2.34 for the notion that traffic data is different under international law than content data.

127. Milanovic, *supra* note 113, at 111 ("I argue that the rules and principles governing the application of the ICCPR and the ECHR should broadly be the same, despite the textual differences in the two jurisdiction clauses."); Deeks, *supra* note 112.

128. Big Brother Watch v. U.K., App. No. 58170/13 Eur. Ct. H.R. 2013419-21 (2018), http://hudoc.echr.coe.int/eng?i=001-186048 [https://perma.cc/B92C-TJZM]; *see also* Robert Chesney, *The 'Big Brother Watch' Ruling on U.K. Surveillance Practices: Key Points from an American Perspective*, LAWFARE (Oct. 9, 2018), https://lawfareblog.com/big-brother-watch-ruling-uk-surveillance-practices-key-points-american-perspective [https://perma.cc/7SLR-SVTC].

129. Big Brother Watch, App. No. 58170/13 Eur. Ct. H.R., ¶ 307.

ciple of legality) is satisfied when a statute describes to satisfaction "[(a)] the nature of offences which may give rise to an interception order; [(b)] a definition of the categories of people liable to have their communications intercepted; [(c)] a limit on the duration of interception; [(d)] the procedure to be followed for examining, using and storing the data obtained; [(e)] the precautions to be taken when communicating the data to other parties; [(f)] the circumstances in which intercepted data may or must be erased or destroyed . . . [(g)] the arrangements for supervising the implementation of secret surveillance measures, [(h)] any notification mechanisms and [(i)] the remedies provided for by national law."[130]

The second prong of the standard requires that the aim of the statute be "necessary in a democratic society.[131] Unlike the parsimonious test above, this element of Article Eight codifies the judgment of the court as to whether the degree of interference exceeds what the goal requires,[132] recalling the "least invasive" inquiry, above.

This Note stops short of applying any of the various tests, above, to the H.A.C.C.S. outlay. But it recognizes that these developments offer a set of considerations for developing new surveillance technologies though it falls far short of giving governments a clear picture of what they may or may not do.[133]

Does the substantive law in this field provide the state that wishes to vindicate its rights in cyberspace with sufficient notice of what measures will be lawful? Do these standards meet their own test for foreseeability? Or must defense professionals guess at whether and how international bodies will challenge the design of cyber tools if not their authority to use them? For example, will a botnet-management tool be non-arbitrary because it has a "specific targeted objective" for surveillance or because it is "the least intrusive instrument" available?[134] The H.A.C.C.S. proposal, for instance, simultaneously would not have a specific target as it autonomously monitors traffic data. It is, likely, a much less intrusive instrument than most management techniques as it does not put communications in front of human users' eyes.

130. *Id.*

131. *Id.* ¶ 308.

132. *Id.*

133. Robert Chesney remarks that "[w]hether [Article Eight's doctrinal framework] actually provides predictability—as opposed to masking judicial discretion to pursue policy preferences in either direction—is debatable." *See* Chesney, *supra* note 128.

134. U.N. Human Rights Council, Gen. Cmt. 27, U.N. Doc CCPR/C/21/Rev.1/Add.9, ¶ 14 (Nov. 1, 1999) (interpreting Article 12 of the I.C.C.P.R.'s requirement that restrictions on freedom of movement be permissible, necessary, and proportional (i.e., non-arbitrary)).

Some scholars have argued that the better way forward is by establishing procedural norms that better cognize the technological pitfalls of signals surveillance without stifling nations working in good faith toward the mutual goals of the global community. James Baker, speaking at M.I.T. about artificial intelligence and national security law, admonished his audience: "Don't respond in this area with substance; respond with process."[135] Professor Ashley Deeks writes that "new international norms . . . should be procedural . . . because a consensus about procedural norms is easier to achieve in the context of secret activity, and because a focus on procedural norms will allow states to avoid . . . contentious discussions about their disparate views on . . . privacy."[136]

In her article, "An International Legal Framework for Surveillance," Professor Deeks lists six "procedural norms" that states should adopt when developing new technologies in the burgeoning field of signals intelligence.[137] She describes procedural norms as those that "regulate the kinds of procedural protections that states should impose on their own intelligence collection, rather than offer substantive definitions of what areas of personal activity are entitled to privacy and the situations in which states may interfere with that privacy."[138] These norms have the benefit of being objectively verifiable, clear in their meaning, and familiar in that they may be drawn from a nation's own laws.[139] Her list consists of (a) legality/notice; (b) limits on reasons to collect or query data; (c) periodic review of surveillance authorization; (d) limits on retention of data; (e) preference for domestic action; and (f) neutral oversight bodies.[140] These notions should be familiar.

These norms capture many of the restraints courts ultimately impose on these technologies when applying substantive law. In *Big Brother Watch*, the court focused on both the "above the waterline" selection criteria for which communications are reviewed and the oversight of this process.[141] The court reviews the regime's provi-

135. James Baker, *Starr Forum: Artificial Intelligence and National Security Law: A Dangerous Nonchalance*, YOUTUBE at 1:01:10 (Mar. 9, 2018), https://www.youtube.com/watch?v=BVQltGtMIho [https://perma.cc/FKW7-FEB8].

136. *See* Deeks, *supra* note 112, at 295.

137. *Id.*

138. *Id*. at 349.

139. *Id*. at 349–50.

140. *Id*. at 351–63.

141. Big Brother Watch, App. No. 58170/13 Eur. Ct. H.R., ¶¶ 490–95; *see also id*. ¶¶ 375–83 (describing oversight of the warrant process).

sions for when retained information must be destroyed and requires that bodies provide for a periodic review-stored data to determine whether its retention remains necessary.[142] The court also acknowledges the program's requirement that authority be reviewed periodically and that warrants be updated.[143]

Where the court finds procedures to be deficient, however, it does not outline what would satisfy the various substantive requirements it applies. In a confounding moment, the court, finding that there is no evidence of abuse in the selection process or the metadata-search process, both overseen by the Interception of Communications Commissioner, concludes that there is not enough oversight to prevent abuse.[144] Unhelpfully, the opinion does not reach what quantum of oversight would permit the state to enact the program. For states acting in good faith to disrupt adversary organizations, this amounts to "guess again" on the issue of countermeasure design.

A review that led with process, however, would begin where the "ponderous" 85,000+-word opinion loses steam.[145] The ultimate question, there, would be "what is sufficient?" rather than "what is insufficient?" The *Big Brother Watch*'s treatment of these procedural issues suggests that the answers to these questions may provide responders with the outline of a program that optimally balances the interests of security and human rights.

IV. OTHER SOLUTIONS

A. Binding Law – The Council of Europe Convention on Cybercrime

As nations press for new law that suits their interests and responds to the threats they foresee, some commonalities arise. The lead source of international law, here, is the Council of Europe's Convention on Cybercrime ("the Budapest Convention").[146] The convention originated in the beginning of the 21st century with a push by the Council of Europe to harmonize domestic criminal law governing cyberspace within the community of nations and to promote

142. *Id*. ¶¶ 370–74.

143. *Id*. ¶¶ 358–60.

144. *Id*. ¶ 347.

145. *See* Chesney, *supra* note 128.

146. Convention on Cybercrime, Nov. 23, 2001, E.T.S No. 185 [hereinafter Budapest Convention]. The Budapest Convention is the only binding source of law on cybercrime in international law.

mutual assistance in information sharing and investigative authority.[147] Since then, more than sixty nations have acceded to the document.[148] The document imposes obligations on signatory nations that harmonize substantive and procedural laws. The convention requires that signatories enact legislation establishing a procedural framework for mutual legal assistance with evidence,[149] extradition,[150] jurisdiction,[151] and preservation of evidence.[152]

The Budapest Convention is—from the outset—a more useful source of law than the I.C.C.P.R. for nations seeking guidance on solutions in cyberspace by offering negotiated-for procedural provisions.[153]

A number of these provisions bear directly on the issue of botnet management. The document provides for a permissive regime of traffic-data sharing for communications between signatories.[154] This provision affirms the notion that viewing traffic data—unopened packets—interferes less with privacy interests than viewing content data does.[155] For both data streams, the document provides that nations should share such data in real time according to domestic law,[156] but the document sets a minimum for traffic-data sharing.[157]

147. Jonathan Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, 40 MONASH U. L. REV. 698 (2014).

148. Currently, sixty-two nations have ratified or acceded to the document. Four others have signed without ratifying. COUNCIL OF EUR., CHART OF SIGNATURES AND RATIFICATIONS OF TREATY 185 (2019), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=82mGI8eu [https://perma.cc/M839-7ZE9]. Furthermore, former non-signatories are feeling increasing pressure to join. *See* Rahul Tripathi, *Home Ministry Pitches for Budapest Convention on Cyber Security*, THE INDIAN EXPRESS (Jan. 10, 2019), https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/ [https://perma.cc/F6XH-UEKM].

149. Budapest Convention, *supra* note 146, art. 25–27, 31–32.

150. *Id.* art. 24.

151. *Id.*

152. *Id.* art. 29 (describing expedited preservation of stored computer data).

153. Nothing says that we cannot have both. The bodies of law are not mutually exclusive. But it is the position of this Note that where the community of nations seeks to develop advanced solutions to emergent cyber threats while embracing the principles behind the human rights treaties discussed above, it should use the modular, negotiated framework of the Budapest Convention rather than the adversarial and uncertain limitations imposed by the I.C.C.P.R.

154. Budapest Convention, *supra* note 146, art. 30, 33.

155. *Id.* art. 16, 34.

156. *Id.* art. 16.

157. *Id.* art. 17.

There, it provides that "[e]ach Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case."[158] This simple procedural provision—easily understood and mutually binding—guides engineers toward effective designs that meanwhile protect substantive privacy interests.[159] In this way, defense practitioners can work toward solutions to transnational problems with confidence that their efforts will not incur an unforeseen price.[160]

In addition to the procedural provisions in the document, the Budapest Convention requires that participating nations criminalize certain online behavior within the broad spectrum of (1) "[o]ffences against the confidentiality, integrity, and availability of computer data and systems,"[161] (2) "computer-related offenses,"[162] (3) "content-related offenses,"[163] and (4) "criminal copyright infringement."[164]

There is no mention of botnets in the substantive provisions of the Convention. This would seem to evince the James Baker/ Ashley Deeks issue—that substantive law succumbs to obsolescence more quickly than procedural law.[165] But the convention foresaw this issue. By explaining criminal activities at a high level of abstraction, crimes unforeseen by the writers could be described in the terms defined in the document and agreed upon by parties.[166] Through the hard work of the members involved, the Council of Europe has begun to offer guidance on novel criminal activity as it develops.[167] In

158. *Id.* art. 33(2).

159. Deeks, *supra* note 112, at 350 (explaining that procedural norms can assist in applying substantive law to surveillance).

160. Just as the notice function of the principle of legality in human rights law gives private citizens confidence that their actions will not cause them to suffer, these positive guidelines will encourage nations to develop transparent solutions in cyberspace.

161. Budapest Convention, *supra* note 146, ch. II, § 1, tit. 1.

162. *Id.* ch. II, § 1, tit. 2.

163. *Id.* ch. II, § 1, tit. 3

164. *Id.* art. 10.

165. Baker, *supra* note 135 ("Respond with process, because law will always chase technology. The law never can keep up with Moore's law.").

166. Eur. Consult. Ass., *Explanatory Report to the Convention on Cybercrime* ¶ 36 ("Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.").

167. In 2012, the Cybercrime Convention Committee ("T-CY") began publishing Guidance notes "aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in light of legal, policy and technological developments." Eur. Consult. Ass., *Guidance Notes*, https://www.coe.int/en/web/cybercrime/guidance-notes

2013, the council published a guidance note on botnets, describing the technology and suggesting provisions that apply to various crimes it enables.[168]

The substantive guidance that the convention provides and its procedural model for information sharing combine to give security practitioners the notice needed to tailor botnet-management solutions to international legal obligations. In this way, the convention encourages development of solutions to transnational harms while tailoring those solutions to privacy and liberty norms.[169]

B. Soft Law – Procedural Norms and a Duty to Act

In 2009, former U.S. Secretary of Homeland Security Michael Chertoff described the world in terms of the threat posed by terrorists accumulating within sovereign territories and exerting force that mirrored that of states while a number of nations coopted international legal instruments to pressure the United States to "challenge[] everything from its foreign and homeland security policies to its enforcement of purely domestic laws."[170] He posited that rather than pull out of the international liberal order—as some writers had threatened—the United States should encourage nations to recognize that the "modern international order must be predicated on a new principle, under which individual states assume reciprocal obligations to contain transnational threats emerging from within their borders."[171]

Chertoff made this proposal as a corollary to his defense of the consent model of international law—that international law exists because states, by virtue of their sovereignty, are able to bargain for and consent to reciprocal duties.[172] He finds this evident in the inconsistency in areas of law that his opponents consider immutable human rights[173] and the incoherence of "new and expanded funda-

[https://perma.cc/FC4M-YDC8]. Since 2012, T-CY has published ten notes on various subjects. *Id.* (last visited Jan. 10, 2019).

168. *See* Cybercrime Convention Committee, *T-Cy Guidance Note #2*, *supra* note 167.

169. *See* Deeks, *supra* note 112, at 295 (for the notion that procedural norms can effect compliance with substantive privacy values in surveillance technology).

170. *See* Chertoff, *supra* note 87, at 131 (continuing that "[i]n recent years, international lawyers and scholars have sought to subordinate established U.S. laws and even U.S. constitutional provisions to international legal mandates.").

171. *Id.*

172. *Id.*

173. *Id.* at 134 ("Bodies such as the United Nations include member states that often do

mental rights."[174]

Broad accession to the Budapest Convention on Cybercrime—a negotiated and forward-looking treaty arrangement—and the awkward push to apply extant human rights law[175] to cyberspace tracks with these assertions.

A reasonable reader could interpret the Budapest Convention as endowing signatory nations with a positive duty to contain. By first establishing a harmonious body of criminal law, then describing how this law prohibits a novel criminal enterprise, and finally requiring signatory states to either enforce the law against known criminals or to permit participating states to exercise objective jurisdiction over them,[176] the Budapest Convention endows states with what approaches a legal duty to act against the criminal activity it prohibits.

An affirmative duty to contain botnet-enabled attacks is consistent with international law. In United Nations Special Rapporteur, Frank La Rue's 2013 Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression, La Rue explores topics such as how state interference with communications may implicate Article Seventeen of the I.C.C.P.R.,[177] internet as necessary infrastructure,[178] and potential expressive harms.[179] He includes two paragraphs identifying how the threat of DDoS, whether effected by states or otherwise, offend individual rights and noted that "States have an obligation to protect individuals against" such interference.[180] He goes so far as to say that the "positive obligation to pro-

not share a common position and whose values often clash with those of the United States and other democratic states. For example, the U.N. Human Rights Council has passed resolutions urging states to adopt laws combating the 'defamation of religions,' which would prohibit [discussion] protected under the First Amendment of the U.S. Constitution." He continues, citing the second amendment, inconsistent positions on the death penalty, and these nations' internal inconsistency in applying human rights laws.).

174. *Id.* at 135 ("[A]bsent an express treaty or convention, giving international bodies the power to decide what are new and expanded fundamental rights would allow countries to advance nationalist or bloc political agendas under the guise of human rights.").

175. *See* International Covenant on Civil and Political Rights arts. 17, 19, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

176. *See* Budapest Convention, *supra* note 146, art. 22 (describing that nations must adopt measures necessary to establish jurisdiction over the listed offenses and, upon request, must establish jurisdiction over an offender or extradite that person).

177. U.N. Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, ¶¶ 57, 83, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

178. *Id.* ¶¶ 60–66.

179. *Id.* ¶¶ 44–46.

tect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent" recurrence.[181]

A generally recognized, mutually held duty to contain this criminal activity—violation of which would trigger a concomitant power to respond in a partner nation targeted by botnet-enabled cybercrime—would reaffirm both the victim nation's interest in exercising objective enforcement jurisdiction over the attacker and the host nation's sovereignty through recognition of a bargain for an effective response to inherently transnational—and universally violative—crime.[182] Exercise of such a power to respond would likely be constrained by other norms, specifically minimization of exposure to private data,[183] legality and its notice corollary,[184] and data security.[185]

180. *Id.* ¶¶ 51–52.

181. *Id.* ¶ 52.

182. This would also affirm key norms described by Professor Deeks, including review of surveillance authorization and preference for domestic action. *See* Deeks, *supra* note 112, at 358–59. Consider the function of the U.N. Security Council. Often, when the U.N.S.C. authorizes the use of force, it first concludes that the target has failed to meet a duty of nonviolence or that another state—who had a duty to prevent the violence or its effects—had failed to act, authorizing intervention. *See, e.g.*, S.C. Res. 678 (Nov. 29, 1990) (recognizing the failure of Iraq to comply with international law and subsequently authorizing member states to enforce the previous orders of the Security Council by "all necessary means").

183. Professor Deeks writes about the adjacent norm of collection and use limits on surveillance. *See* Deeks, *supra* note 112, at 354. Minimization is also a key component of Title III surveillance in the United States. As this sort of intervention would be permitted by the host nation's consent to what might otherwise constitute a violation of their sovereign right to exclude, reasonable mitigation would rightfully require some degree of protection of native data. This also incorporates Professor Deeks' norm of a limitation on the retention of data.

184. *See* U.N. Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 17(c)–(d), U.N. Doc. A/70/174 (July 22, 2015) [hereinafter Information and Telecommunications Report] (describing procedure for creation and mutual recognition of computer emergency response teams ("C.E.R.T.s"). N.B. the U.S. approach to intervention appears to be out in the open.); *see also* KEROMYTIS, supra note 67, at Slide 33 (signaling that the H.A.C.C.S. program does not intend to operate in secrecy and that "[s]tealth of the agents is not a primary concern of the program.").

185. *See* Mudge, *supra* note 70, at 0:40:50 (explaining that the two most vulnerable fields of coding are quality assurance and data-security software).

C. Next Steps

In recent years, nations have raced to promote their own sets of norms in cyberspace.[186] The sets of norms proposed by the United States cover much of the same ground as those in the procedural provisions of the Budapest convention, especially with regard to information sharing and assistance in investigations.[187] Significantly, the United States' proposal also includes language establishing a duty to combat cyberthreats within their borders while also providing for process by which cyber-capable nations could intervene in the event of an attack that threatens transnational harm.[188] By moving in this direction, the international order may move toward a new equilibrium whereby cyber-action by capable states aggressively counters universally threatening criminal technologies—but does so out in the open—affirming the universal values of notice and privacy of communications.

186. *The United Nations Doubles its Workload on Cyber Norms, and Not Everyone Is Pleased*, COUNCIL ON FOREIGN RELATIONS DIGITAL AND CYBERSPACE POLICY PROGRAM BLOG (Nov. 15, 2018), https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased [https://perma.cc/UC5R-XM56] (pointing to the United States and Russia's competing proposals to the United Nations General Assembly promoting the establishment of certain norms in cyberspace in advance of a creation of a Group of Governmental Experts in cyberspace); *see* U.N. General Assembly, 73d Sess., First Committee, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Draft Resolution, U.N. Doc. A/C.1/73/L.37 (Oct. 18 2018); *see also* U.N. General Assembly, 73d Sess., First Committee, Developments in the Field of Information and Telecommunications in the Context of International Security, Revised Draft Resolution, U.N. Doc. A/C.1/73/L.27/Rev.1 (Oct. 29 2018). Furthermore, the article mentions efforts by the Philippines and France to establish their own sets of norms. *See also* Eichensehr, *supra* note 42, at 322 ("Two opposing visions of cyberspace governance are coalescing: a state-focused, multilateral vision promoted by China and Russia, and a multi-stakeholder vision promoted by the United States and its allies. This fundamental clash about the nature of cyberspace permeates the states' approaches to cyber governance questions and creates a risk of conflict.").

187. Information and Telecommunications Report, *supra* note 184, ¶¶ 9–18. This iteration of the discussion before the general assembly contains the norms that the United States favors for the new Group of Governmental Experts.

188. *Id.* ¶ 13(a), (c), (d), (h); *see also id.* ¶ 17(c)–(d) (providing for procedure by which recognized C.E.R.T.s could exercise a limited power to intervene for a limited period of time in nations affected by botnet activity—again, based on the theory that states have, as an aspect of their sovereignty, acceded to the legal instruments (i.e., the U.N. Charter and Budapest Convention) providing for these legal duties and powers).

CONCLUSION

Cybercrime methods, cybersecurity tactics, and the laws that govern cyberspace have developed in response to one another. But while capabilities of both good and bad actors in cyberspace evolve at the rate of technological advance, international law is necessarily slowed by deliberation and diplomacy. Filling the void with borrowed law from adjacent, pre-cyber fields threatens to leave practitioners in a confidence vacuum leading to the same practice of secrecy and overbroad discretion that left global partnerships strained in the wake of the 2013 surveillance revelations. But by filling the void with negotiated procedural norms and positive law that anticipates advances in technology, the international community can move toward a safer, more transparent internet.

*Grant Gerard**

* J.D. Candidate, Columbia Law School, 2020. I would like to thank Professor Waxman for his guidance in this process and the *Journal* staffers for their hard work and input. I would also like to thank my family for their constant support, as well as Jeb and Jolene.