VOLUME 54 NUMBER 2 2023

THE GEORGE WASHINGTON INTERNATIONAL LAW REVIEW

TABLE OF CONTENTS

ARTICLES

The City's Right to Self-Determination, *Pars Pro Toto*? 179 *Benjamen Franklen Gussen*

The Obligation to Prevent Transboundary Cyber Harm: Expand the Regulatory Regime or Continue Deflecting Responsibility 219 *Dafina Buçaj*

NOTES

Using Uganda as a Model for Regulating Access to and Benefit-Sharing of Biological Resources and Traditional Knowledge in the United Republic of Tanzania 285 *Christina Morgan*

The Copyright Authorship Conundrum for Works Generated by Artificial Intelligence: A Proposal for Standardized International Guidelines in the WIPO Copyright Treaty 311 *Kavya Rallabhandi*

Contracting for Collateral: Solving the Sovereign Bond Enforceability Problem 349 *Victoria Colbert*

Avast, Ye Botnets!: Applying Lessons from the Law of Piracy to the Problem of Botnets 375 *Ryan R. Migeed*

AVAST, YE BOTNETS!: APPLYING LESSONS FROM THE LAW OF PIRACY TO THE PROBLEM OF BOTNETS

Ryan R. Migeed[*]

Abstract

Botnets—collections of computers infected with malware that surreptitiously controls them—steal millions of consumers' banking information for personal profit. To do so, they typically infect computers in multiple States, victimizing citizens of different States and using the Internet infrastructure of various States. Botnets terrorize citizens of every State equally. They are modern-day pirates, using our highways of commerce to rob civilians. In the process, they are destabilizing global commerce. Because the volume of cyber intrusions is so great, some have called for allowing private companies to engage in "hackback" against the hackers—essentially acting as privateers for States that do not have the capacity to protect every civilian. But this creates the risk of undesirable consequences and violates a developing custom against hackback.

This Note compares the problem of botnets to piracy to explore the legal rationales that underpin action against botnets. It analyzes the ways in which States have collaborated to solve the piracy problem and concludes by recommending that States model a U.N.-sanctioned anti-botnet taskforce after the taskforce charged with repressing pirates off the coast of Somalia. Moreover, this Note argues that States should agree not to allow private companies to act as privateers—to engage in hackback—but, rather, should reassert the monopoly of States' police powers in the interest of progressively developing customary international law regarding States' conduct in cyberspace. States should also recognize the use of botnets as international criminal activity and as an illegitimate use of State power as a matter of international law.

Table of Contents

I. Introduction 376
II. Defining the Problem 378
A. Botnets 378
B. Hackback 381
C. Comparing Botnets to Pirates 382
D. Comparing the Jurisdictional Challenges Posed by Pirates and Botnets 384
III. Repressing Piracy under International Law 386

[*] J.D. 2022, The George Washington University Law School; B.A. 2015, American University. The author would like to thank Professors Brandon Jackson, Sean D. Murphy, and Dan Stigall for reviewing prior drafts and offering feedback which has made this Note immeasurably better.

A. From English Municipal Law to UNCLOS........ 386
B. Case Study: U.N.-Authorized Multilateral Anti-Piracy Taskforce................................ 390
IV. Cyber Privateerism as a "Solution" to Cyber Piracy? .. 393
A. Historical Usage (and Denunciation) of Privateers... 393
B. Cyber Privateers Pose the Same Problems as Privateers of Old 396
V. Military Solutions to A Transnational Crime Problem?... 399
VI. Existing International Cooperation Against Cybercrime... 401
A. The Budapest Convention: Coordinating Laws But Not Operations Against Botnets 402
B. The Paris Call's Attempt to Create a "Norm" Against Hackback 403
C. Case Study: Joint Cybercrime Action Taskforce as a Potential Model for Action Against Botnets 404
D. Do Competing Legal Theories Blockade Cooperation in Cyberspace?..................... 405
VII. Defining the Solution: Authorizing Action Against Botnets.. 409
A. U.N. Security Council Authorization and a Three-Part Framework for Confronting Botnets......... 411
B. Toward Customary International Law on Botnets... 417
C. Secondary Benefits: Promoting Attribution and Deconfliction................................... 421
VIII. Conclusion 422

I. Introduction

On October 12, 2020, Microsoft announced that, pursuant to a court order,[1] Microsoft and a number of telecommunications providers from around the world had disrupted the infamous Trickbot botnet.[2] A botnet is a collection of computers that have been

[1] Microsoft Corporation v. John Does 1-2, No. 1:20-cv-1171 (AJT/IDD) (E.D. Va. Oct. 20, 2020) (order granting preliminary injunction).

[2] *See* Tom Burt, *New Action to Combat Ransomware Ahead of U.S. Elections*, Microsoft (Oct. 12, 2020), https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/ [https://perma.cc/ZG6N-GQ3Z]. Microsoft's coordinated effort included Slovakia-based security firm ESET, the Financial Services Information Sharing and Analysis Center, NTT, Lumen's Black Lotus Labs, and Symantec. *See* Shannon Vavra, *Cyber Command, Microsoft Take Action Against TrickBot Botnet Before Elec-*

infected by malicious software ("malware") that surreptitiously controls the machines, turning them into a robot army for whoever controls the botnet.[3] Trickbot is a collaborative of an unknown number of cyber criminals who use their botnet—some two million computers[4] remotely controlled by Trickbot's servers—to infect networks with ransomware.[5]

Trickbot is emblematic of the latest trend in cybercrime: botnets are big business, offering the computers under their control to conduct cyberattacks or digital bank robberies on behalf of the highest bidder.[6] For as little as $20, one service offers a botnet powerful enough to take a website offline through a distributed denial of service (DDoS) attack.[7] In a DDoS attack, the controller orders each of the computers in the botnet to simultaneously send requests to a web server.[8] Though this can be as simple as millions of computers trying to access a website, the amount of traffic can overwhelm the server and cause the website to "crash," or become unusable.[9]

The effort to disrupt Trickbot was spearheaded by Microsoft's Digital Crimes Unit, which—despite its name—has no legal jurisdiction as a law enforcement entity. Microsoft's civil claim against Trickbot in the U.S. District Court for the Eastern District of Virginia is not the first time Microsoft has won a court order to disable a botnet; in fact, the company pioneered the "litigation response to botnets" as early as 2010, when the same court permitted Microsoft to disable the Waledac botnet (albeit under the supervision of U.S.

tion Day, CYBERSCOOP (Oct. 12, 2020), https://www.cyberscoop.com/trickbot-takedown-cyber-command-microsoft/ [https://perma.cc/MJY4-3DVL].

[3] *See* Mark Bowden, *The Enemy Within*, THE ATLANTIC (June 2010), https://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/308098/ [https://perma.cc/8JTQ-NBNS].

[4] *See Attacks Aimed at Disrupting the Trickbot Botnet*, KREBS ON SECURITY (Oct. 2, 2020, 2:20 PM), https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/ [https://perma.cc/N3E7-55RE] (estimating the number of computers controlled by Trickbot).

[5] Ransomware is malware that locks a victim's computer—or threatens to publish data stored on it—unless the victim pays a ransom. *See* U.S. CYBERSPACE SOLARIUM COMM'N, Report at 137(2020) [hereinafter SOLARIUM COMM'N].

[6] *See* Burt, *supra* note 2.

[7] Rommel Joven & Evgeny Ananin, *DDoS-for-Hire Service Powered by Bushido Botnet*, FORTINET (Oct. 26, 2018), https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet- [https://perma.cc/PR2H-PC86].

[8] *See* P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 44 (2014).

[9] *See* Bowden, *supra* note 3.

Marshals).[10] While the disruption of a predatory botnet was cause for celebration, such interference raises the question of which entity should be in charge of responding to such threats to citizens' privacy and pocketbooks. Notably, Microsoft's Trickbot action came a couple of days after an operation against Trickbot by U.S. Cyber Command (CYBERCOM).[11] How much should private corporations be allowed to enforce against harmful cyber actors like botnets—and how much more enforcement should government entities like CYBERCOM be doing?

This Note is divided into seven Parts. Part II defines the problem, addressing the scope of botnets' harm to global commerce and comparing that harm to the piracy that threatened the free flow of commerce on the high seas in the 18th and 19th centuries. Part III discusses the international conventions that denounce piracy, and Part IV assesses privateerism—also known in the cyber context as "hackback"—as a potential solution to cybercrime, which has gained some traction in the literature. Part V briefly discusses how transnational crime has been treated as a military problem. Part VI then evaluates current international opinion and frameworks attempting to achieve international cooperation on cybercrime. Noting that existing frameworks fall short, Part VII proposes the creation of a global taskforce to combat botnets and discusses how such a taskforce could solve the instant problem as well as begin to achieve more permanent cyber norms.

II. Defining the Problem

A. *Botnets*

A botnet is formed when an actor infects multiple computers with malware that takes control of those computers, allowing the actor to leverage the computing power and network access of the machines without their owners knowing they have been breached.[12] Control is exercised by the "command-and-control" server, through which the malicious actor sends commands to the computers.[13] Using this network of so-called "zombie" computers,

[10] *See* Grant Gerard, *Botnet Mitigation and International Law*, 58 Colum. J. Transnat'l L. 189, 206 (2019) (citing Complaint at ¶¶ 34–39, Microsoft Corp. v. John Doe, No. 1:10-cv-00156 (E.D. Va. Feb. 22, 2010)).

[11] *See Microsoft Uses Trademark Law to Disrupt Trickbot Botnet*, Krebs on Security (Oct. 12, 2020, 8:52 AM), https://krebsonsecurity.com/2020/10/microsoft-uses-copyright-law-to-disrupt-trickbot-botnet/ [https://perma.cc/368V-W6A4].

[12] Singer & Friedman, *supra* note 8, at 44.

[13] *See* Bowden, *supra* note 3.

the controller can spread malware far and wide or launch a DDoS attack.[14] The threat of a DDoS attack can also be used to extort ransoms from companies who do not want to suffer the economic losses from having their services rendered inaccessible to customers for a period of time.[15] In this way, botnets can be both a threat in themselves (essentially the infrastructure of an organized criminal gang) and one of several tools wielded by an actor (such as a State) to accomplish certain goals.[16]

A cursory glance through any major cybersecurity firm's online threat reports makes clear the growing ubiquity of botnets.[17] Estimates suggest that nearly a third of all Internet traffic is due to botnet activity, most of it in DDoS attacks,[18] and a fourth of all the computers used worldwide may at one point have been linked to a botnet.[19] The problem has become particularly acute during the COVID-19 pandemic as millions of people worked from home on insecure networks and cybercriminals used pandemic fears to spread malware under the guise of providing pandemic-related information.[20] And, as more WiFi-connected gadgets come onto the market—the so-called "Internet of Things"[21]—botnets are given more opportunities to spread to routers that control Internet access for the growing number of devices in the modern home.[22]

[14] *See* Singer & Friedman, *supra* note 8, at 44.

[15] *See* Chuck Easttom, Computer Security Fundamentals 111 (4th ed. 2020).

[16] *See* Bowden, *supra* note 3.

[17] *See, e.g.*, SecureList, http://www.securelist.com [https://perma.cc/3QW9-EGSC] (Kaspersky Labs' index of threat reports); *Threat Intelligence Reports*, FireEye https://www.fireeye.com/current-threats/threat-intelligence-reports.html [https://perma.cc/ZE5J-XNPV] (FireEye's database of threat reports).

[18] *See* Solarium Comm'n, *supra* note 5, at 87.

[19] *See* Bowden, *supra* note 3.

[20] *See INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19*, Interpol (Aug. 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 [https://perma.cc/UQ4W-A77Z]. The Cyber Security Agency of Singapore reported a three-fold increase in the number of "zombie" computers during the pandemic. Kenny Chee, *Big Jump in 'Zombie' Devices Laced with Malware*, The Straits Times (July 9, 2021), https://www.straitstimes.com/singapore/big-jump-in-zombie-devices-laced-with-malware (last visited Nov. 4, 2022).

[21] This includes wireless devices such as printers, home security systems, and thermostats, which can all be coopted by a botnet because they are connected to the Internet via a home WiFi network. These devices also have much weaker cybersecurity protections than the average computer, making them an easy entry-point into a WiFi network for a botnet looking to ensnare more computers. *See What Is the Internet of Things (IoT)?*, Cloudflare, https://www.cloudflare.com/learning/ddos/glossary/internet-of-things-iot/ (last visited Mar. 1, 2021).

[22] *See, e.g.*, *What Is the Mirai Botnet?*, Cloudflare, https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (last visited Jan. 24, 2021).

The Spamhaus Project, an international nonprofit organization that tracks botnets and other cyber threats, identified a 71.5 percent increase in the number of "command-and-control" servers hosting botnets from 2018 to 2019.[23] The servers controlling these botnets are located in countries across the globe, with Russia, the United States, the Netherlands, and China ranking as hosts to the most botnet controllers, respectively.[24] While most of these botnets' activity is focused on stealing consumers' log-in credentials to commit online-banking fraud, Spamhaus has observed the threat actors increasingly evolving their methods toward what Spamhaus calls a "Pay-Per-Install model."[25] For a fee, controllers of a botnet offer other cybercriminals access to the infected machines under their control to wreak whatever havoc they so choose—a growing trend among cybercriminals to offer crime itself as a service.[26]

Botnets are a unique threat to global commerce and national security, affecting consumers and companies all over the world.[27] A U.S. Congressional commission established to evaluate modern cyber threats singled out botnets, recommending that the United States strengthen its ability to disable them and warning that "[b]otnets could hijack billions of devices to disrupt entire regions, creating new national security challenges."[28] Meanwhile, in raw economic terms, a botnet of 30,000 bots can generate over $18 million in bank fraud per month.[29] Having already lost millions of dollars due to botnet attacks, companies are understandably eager to end the financial bloodletting.[30] The increase in financial casualties has led to a spirited debate among companies, regulators,

[23] *See Spamhaus Botnet Threat Report 2019*, Spamhaus (Jan. 28, 2020, 6:36 PM), https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019 [https://perma.cc/9BGY-KRG2].

[24] *Id.*

[25] *Id.*

[26] *See* Burt, *supra* note 2 (referring to this as "malware-as-a-service" when the "customer" uses the botnet to spread malware).

[27] *See* Solarium Comm'n, *supra* note 5, at 17.

[28] *Id.* at 17, 87.

[29] *See Inside the Business Model for Botnets*, MIT Tech. Rev. (May 14, 2018), https://www.technologyreview.com/2018/05/14/142895/inside-the-business-model-for-botnets/ [https://perma.cc/DGP6-MUY5].

[30] *See, e.g.*, The Council of Econ. Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy 8–13 (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/LAX4-A6SQ] (finding that DDoS attacks are the second-most damaging cyber-enabled event following intellectual property theft and that firms lose on average about 0.8 percent of their market value in markets' reactions to the news of a cyber-related event affecting the company alone).

and commentators about the extent to which private actors should be permitted to use their own cyber capabilities in hackback against botnets.[31]

B. *Hackback*

"Hackback" is the term given to the ways in which companies (could) electronically follow hackers back to their lairs, either to identify them for law enforcement or to disrupt their systems and prevent them from hacking again.[32] Some take a broad view of what is included in hackback.[33] This Note does not. Here, use of the term hackback is limited to events like the Microsoft-led disruption of Trickbot—instances in which a private actor degrades a hacker's system to an extent that reduces or eliminates the system's capability to continue hacking. This definition of hackback does not include methods used merely to identify hackers, which do not harm the hackers' systems. Examples of such methods include beaconing[34] and the use of honeypots.[35]

Hackback could be sanctioned by governments, just as privateers were once permitted to attack enemy ships under State authority. However, many States came to disfavor high seas privateers after criminalizing piracy.[36] To combat the problem of pirates—a threat to companies' profit margins and innocent civilians—States turned to interstate cooperation schemes, not privateers. Thus, historical experiences with both pirates and privateers provide lessons for how best to combat botnets today.

[31] *See, e.g.*, Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, THE ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ [https://perma.cc/2WRW-W9K7].

[32] FireEye is one firm that has publicly admitted to "hacking back." *See* Scott J. Shackelford et al., *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 U. PA. J. INT'L L. 377, 382 (2019).

[33] *See, e.g.*, *id.* at 389-90.

[34] Beaconing is the process of sending to another computer a file which, when opened, transmits data about the receiver, usually including IP address, back to the sender. *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 1, 11 (2014).

[35] A honeypot is a computer system designed to look unprotected so that it attracts hackers who can then be caught in the act or traced back to their IP address. *See id.* at 18.

[36] *See* discussion in Section IV *infra*.

C. *Comparing Botnets to Pirates*

This is not the first analysis to find the comparison of the actions of cybercriminals to pirates useful.[37] As one legal scholar wrote, "this analogy is attractive for many reasons."[38] Not least of these reasons are the facts that cyberspace functions as "a highway of commerce" similar to how sea routes bring goods to market, and that hackers enter computers to steal data in a way logically similar to how pirates board vessels to steal cargo.

As cyber threats go, botnets are *particularly* analogous to pirates. Like pirates, who take advantage of police-less international waters, botnets pose an enforcement problem because they operate in the "ungoverned badlands" beyond any one state's control.[39] This "jurisdictional lack of clarity" allows online threats like botnets to multiply.[40] The problem is exacerbated by uneven enforcement: not all States enforce their anti-hacking statutes as aggressively as States such as the United States does through its Department of Justice.[41]

The threat of a major ransomware or DDoS attack perpetrated by a botnet also adds tremendous costs to businesses that use the Internet to provide goods and services.[42] Just as the threat of pirates holding shipping containers captive in the Gulf of Aden has driven up insurance rates for shipping firms and resulted in "specific insurance products to address piracy-related ransom costs,"[43]

[37] *See, e.g.*, Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 Stan. J. Int'l L. 103, 110 (2014); Singer & Friedman, *supra* note 8, at 177.

[38] Rosenzweig, *supra* note 37, at 110.

[39] Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, Strategic Stud. Q. 32, 44 (Spring 2011).

[40] *Id.* at 43.

[41] *See Spamhaus Botnet Threat Report 2019*, *supra* note 23; *see also, e.g.*, Press Release, U.S. Dep't of Just., Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally (Sept. 16, 2020), https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer [https://perma.cc/25FD-A4Y5]; Press Release, U.S. Dep't of Just., Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and [https://perma.cc/F73D-5J77].

[42] *See* The Council of Econ. Advisers, *supra* note 30.

[43] Lauren Ploch et al., Cong. Rsch. Serv., R40528, Piracy off the Horn of Africa 14 (2011), https://fas.org/sgp/crs/row/R40528.pdf [https://perma.cc/R7UE-TMSC].

the threat from online attackers like botnets has produced a new industry of cyberattack insurance providers.[44]

Moreover, just as pirates sailed under false flags of States or no identifying flag at all, botnets can hide their country of origin or even the fact that they may be operating on behalf of a State.[45] As one researcher has noted, "[t]racing back through the attacking machines to find the actual source of an attack may involve several stages through multiple machines in different jurisdictions," adding "complexity and delay" to dismantling botnets.[46] This anonymity is why one of the most persistent difficulties in deterring cyber attackers generally, and botnets especially, is being able to accurately attribute their attacks to them in the first place.[47]

History shows that the ways in which botnets are pursued also parallel the ways in which States have pursued pirates. States try to catch and prosecute them. As in the case of Microsoft, at least one State has, through its courts, condemned botnet property and permitted a private actor to dismantle the offender's infrastructure. As discussed below in Part IV, this outsourcing of the State's police power spawned problems of its own—a harbinger of things to come if States continue to rely on private companies to defeat botnets for them.

The most readily apparent critique of this comparison is that getting online is not simply setting sail in a vast, unclaimed territory. However, anyone with a laptop can connect to WiFi in many countries—and, once connected to the Internet, can navigate it freely without territorial restraints. And, although the Internet requires cables, modems, and servers which are within the territories of States, sea trade requires infrastructure just as virtual commerce does: ports and shipbuilding capability, as well as the establishment of sea lanes and, today, a host of regulations covering ship safety, among other things.[48] These foundations, like cyber infrastruc-

[44] *See* Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem [https://perma.cc/4ZA2-EWXF].

[45] *See* Wajeeha Ahmad, *Why Botnets Persist: Designing Effective Technical and Policy Interventions*, MASS. INST. TECH. INTERNET POL'Y RSCH. INITIATIVE 1, 6 (2019), https://internetpolicy.mit.edu/wp-content/uploads/2019/09/publications-ipri-2019-02.pdf [https://perma.cc/JB45-K88F].

[46] *Id.*

[47] *See* SOLARIUM COMM'N, *supra* note 5, at 27; *see also* SINGER & FRIEDMAN, *supra* note 8, at 72–74 (explaining the "problem of attribution").

[48] *See, e.g.*, International Convention for the Safety of Life at Sea (SOLAS), Nov. 1, 1974, 32 U.S.T. 47, 1184 U.N.T.S. 278.

ture, are State investments which the States undoubtedly want to maintain.

Botnets, then, are a classic "tragedy of the commons," in which "the security so vital to all Internet users remains the responsibility of none."[49] The Internet—just like the high seas—is available for everyone to use. Because it is a common resource, any hazard that endangers its common use requires collective action.[50]

Although some States have a treaty obligation under the U.N. Convention on the Law of the Sea (UNCLOS) to cooperate in repressing piracy on the high seas, as discussed *infra*, States do not have obligations to act in an area—like cyberspace—that is "unregulated by international law."[51] The *Lotus* principle in international law presumes freedom of State action except where States' actions are specifically restricted by treaty or customary international law.[52] The question of *whether* States have an obligation not to use botnets to commit cyberattacks on other States is beyond the scope of this Note. Rather, the question posed here is whether the practice of States to dismantle botnets can be formed such that it *will become* an obligation of States to cooperate on disrupting botnets in the same way that an obligation to repel pirates arose in customary international law.

D. *Comparing the Jurisdictional Challenges Posed by Pirates and Botnets*

Jurisdiction is key to answering the question of what legal options exist under international law to enable States to dismantle

[49] Letter from Mark Warner, U.S. Sen., to Tom Wheeler, Chairman, Fed. Commc'ns Comm'n (Oct.25, 2016), https://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CD1BBB25-83E0-494D-B7E1-1C350A7CFCCA [https://perma.cc/Q2K5-HCRH].

[50] *See Senator Prods Federal Agencies on IoT Mess*, Krebs on Security (Oct. 25, 2016), https://krebsonsecurity.com/2016/10/senator-prods-federal-agencies-on-iot-mess/ [https://perma.cc/2DMK-MXKV].

[51] Gary P. Corn, *Cyber National Security: Navigating Gray-Zone Challenges in and Through Cyberspace*, draft prepared for publication in Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare 48 (Michael N. Schmitt et al. eds., 2019) (citing Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 85 (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017) (internal quotation marks removed), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071 [https://perma.cc/9H8F-RZ85].

[52] *See id.* at 49; *see also* The Case of the S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 ("International law governs relations between independent States. The rules of law binding upon States . . . emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law. . . . Restrictions upon the independence of States cannot therefore be presumed.").

botnets because jurisdiction limits States' ability to act. States may claim jurisdiction in one of three ways: to prescribe (or "make law"), to adjudicate (or "apply law"), and to enforce (or "compel compliance with law").[53] A State has jurisdiction to prescribe law with respect to four types of offenses: conduct that takes place within its territory, activities of its nationals outside of its territory, acts outside its territory that have substantial effect within its territory, and conduct outside its territory directed against the security of the State.[54] In practice, enforcement of such laws is more limited than might be assumed; extraterritorial enforcement jurisdiction is "tightly constrain[ed]" under international law, and a State must obtain permission prior to exercising such law enforcement functions in another State's territory.[55]

To fully appreciate the comparison between pirates and botnets, and why similar legal tools might be transposed from one to the other, it is necessary also to understand broadly how Internet traffic works. Communications—sent by computers in a botnet or any regular consumer's computer—are split up into their component parts so that Internet traffic can travel more efficiently.[56] These parts, called "packets," are reconstituted into the whole when they reach the receiving computer. In transit, packets may have traveled through multiple servers in multiple States. The territorial application of the international law of piracy is limited to "place[s] outside the jurisdiction of any State."[57] But is the law's potential reach different, practically speaking, when it comes to a botnet made up of bots in multiple States, evading detection by bouncing its Internet Protocol (IP) Addresses across multiple States, and harming citizens of multiple States in the process? When so many States can claim jurisdiction, is not the *practical* effect—that the

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

[54] *Id.* § 402. States may exercise jurisdiction to enforce these offenses where they have jurisdiction to prescribe them. *Id.* § 431.

[55] Dan E. Stigall, *Ungoverned Spaces, Transnational Crime, and the Prohibition on Extraterritorial Enforcement Jurisdiction in International Law*, 3 Notre Dame J. Int'l & Comp. L. 1, 11, 16 (2013); *see also* Restatement (Fourth), *supra* note 53, § 432(b) ("[A] state may not exercise jurisdiction to enforce in the territory of another state."); *cf.* Stigall, *supra* note 55, at 11–16 (discussing history of extraterritorial exercise of enforcement jurisdiction prior to 1933, which "was not always characterized by tight constraints").

[56] It takes less bandwidth to transfer a piece of a video, for instance, than the whole video at once. "Packet-switching" is the name given to this process of enabling Internet users to share network resources so that they can access content more quickly. *See* Singer & Friedman, *supra* note 8, at 17–18.

[57] U.N. Convention on the Law of the Sea, art. 101, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994) [hereinafter UNCLOS].

broad overlap of jurisdiction renders the activity "outside the jurisdiction of any [particular] state"—the same? And should the first State able to dismantle the botnet not have the right to do so?

Botnets pose a unique problem not only to individual states but potentially to international order. They are essentially criminal gangs, which can have the effects of States but are not States. Moreover, botnets evade coordinated international law enforcement by taking advantage of weak States which are either unable to dislodge them or too afraid to do so given the potential economic and political consequences.[58] The question presented, then, is what legal rationale exists under international law to enable States, either unilaterally or in coordination with each other, to dismantle botnets?

III. Repressing Piracy under International Law

A. *From English Municipal Law to UNCLOS*

The earliest modern effort to pursue pirates and prosecute them for their activities was in 1511, when King Henry VIII of England commissioned John Hopton to "seize and subdue all . . . pirates, exiles, and outlaws . . . and to bring all . . . into one of [England's] ports."[59] Under English municipal law, two essential elements of the crime of piracy helped distinguish it from other crimes: first, the accused had to be "acting for private motives (*animo furandi*)," and second, the accused had to act equally "against all lucrative targets . . . and not the vessels of one flag or a narrowly prescribed group of allied flags."[60] This second element rendered pirates *hostis humani generis*, or "enemies of all mankind," and piracy a crime against all nations.[61] Pirates were also distinguished from non-pirates by the fact that they acted without a commission from a

[58] As discussed in Section VI.D *infra*, mounting publicly available evidence demonstrates that Russia passively permits botnets in its territory as long as Russian citizens are not victimized, and may even actively coordinate with a botnet. Data breaches—which hurt consumers' as well as businesses' bank accounts—in an already weak economy could destabilize a regime which has staked its longevity on economic growth and foreign policy successes. *See* Timothy Frye, *Russia's Weak Strongman: The Perilous Bargains that Keep Putin in Power*, 100 Foreign Affs. 116, 120–121 (May/June 2021).

[59] Alfred R. Rubin, The Law of Piracy 36 (1988).

[60] *Id.* at 82 (internal quotation marks omitted).

[61] *See* Jordan Wilson, *The Rise, the Fall, and the Eventual Return of Modern Piracy: Addressing an Age-Old Problem with Modern Solutions*, 47 J. Mar. L. & Com. 297, 313 (2016). This second element of the crime of piracy has classical roots in the law of war as understood by the Roman Empire, which treated as "*pirata*" those who "did not declare 'war' before their attacks, and attacked all with whom they were not in treaty relationships or who were too strong to beat." Rubin, *supra* note 59, at 83. *See also* Terence Fokas, *The*

sovereign to seize enemy ships or goods; however, this was primarily relevant in wartime, and even those sailors who exceeded their commissions were not necessarily tried as pirates.[62]

The element of *hostis humani generis* had the effect of extending enforcement of English criminal law across the high seas.[63] Still, because they were a common concern to all States, pirates generally came to be viewed under a "universality principle" of jurisdiction; whereas States' jurisdiction is usually limited to conduct within their territories, or conduct committed by a national, or a harm suffered by a national, universal jurisdiction can be exercised on the premise that "certain offenses are so egregious that any state can invoke jurisdiction on behalf of the world community to punish and deter the criminal."[64] The universality principle solved the jurisdictional challenges of prosecuting pirates, namely, States' desire to shield their own nationals from prosecution and some States' lack of resources needed to assert jurisdiction over a pirate.[65]

The suppression of piracy became a political and military goal of the United Kingdom in the early 1800s, when "political pressures" compelled British political leaders to develop a legal rationale for naval action "against those who . . . interfered with British merchant shipping in the Mediterranean Sea."[66] Later, under the Nyon Agreement of 1937 among nine European States, Britain and France were given "special policing authority" in the Mediterranean Sea to destroy submarines "believed to have attacked neutral merchant vessels."[67] Rather than conferring universal jurisdiction on States to apply laws against piracy, Professor Rubin noted, refer-

Barbary Coast Revisited: The Resurgence of International Maritime Piracy, 9 U.S.F. MAR. L.J. 427, 436–37 n.59 (1997).

[62] *See* RUBIN, *supra* note 59, at 95–96, 98–99 (describing Captain William Kidd's commissions and subsequent trial for exceeding a commission); *cf. id.* at 238 (a British legal opinion in 1854 retained the "without any lawful Commission" element of the definition of piracy). Thus, the branding of the Barbary States as "pirates" was mere political rhetoric, as they commissioned privateers in precisely the same way that English kings did, *id.* at 18, which commissions were recognized as valid sovereign acts by English courts, *id.* at 202 n.9, and "the normal laws of war" between sovereigns were observed in conflicts with the Barbary States. *Id.* at 154.

[63] *Id.* at 86–89.

[64] Fokas, *supra* note 61, at 436–37; *see also* Int'l Law Comm'n, Rep. to the General Assembly on the Work of Its Fifty-Eighth Session, 61 U.N. GAOR Supp. No. 10, at 522-23 ¶ 16, U.N. Doc. A/61/10 (2006) (explaining that universal jurisdiction is exercised by a state on behalf of the international community, not "exclusively in its own national interest").

[65] *See* Fokas, *supra* note 61, at 433.

[66] *See* RUBIN, *supra* note 59, at 212.

[67] *Id.* at 295–97.

ence to "piracy" as a legal category in such agreements seemed to be aimed at conferring "political rights to impose order on the high seas in the interests of general commerce."[68]

At its seventh session, in 1955, the International Law Commission commenced a process for codifying and progressively developing the law of the sea, including customary international law applicable to piracy.[69] Rules of customary international law are formed by a general practice of States in conjunction with *opinio juris*, meaning that States view the practice as pursuant to a legally binding obligation.[70] In its commentary to Article 38 of its final draft articles on the law of the sea, an article that would later be adopted as part of Article 14 of the 1958 Convention on the High Seas, and then as Article 100 of UNCLOS, the Commission concluded that States have a duty under customary international law to repress maritime piracy: "Any State having an opportunity of taking measures against piracy and neglecting to do so, would be failing in a duty laid upon it by international law."[71] States are not without discretion in meeting this duty, as the Commission noted that "the State must be allowed a certain latitude as to the measures it should take to this end in any individual case."[72]

Under Article 100 of UNCLOS, all States Parties have a duty to "cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State."[73] Piracy is defined in UNCLOS, in part, as "any illegal acts of violence or detention . . . committed for private ends by the crew or the passengers of a private ship" that occur "on the high seas" or "in a place outside the jurisdiction of any State."[74] Perhaps most relevant to the botnet comparison is the definition of a pirate ship or aircraft in Article 103:

> A ship or aircraft is considered a pirate ship or aircraft if it is intended *by the persons in dominant control* to be used for the purpose of committing one of the [defined acts of piracy]. The

[68] *Id.* at 297.

[69] *Report of the International Law Commission to the General Assembly*, 10 U.N. GAOR Supp. No. 9, at 20, U.N. Doc. A/2934 (1955), *reprinted in* [1955] 2 Y.B. Int'l L. Comm'n 19, U.N. Doc. A/CN.4/SER.A/1955/Add.l.

[70] *See* Int'l Law Comm'n, Rep. on Its Seventieth Session, U.N. Doc. A/73/10, at 119 (2018).

[71] *Report of the International Law Commission to the General Assembly*, 11 U.N. GAOR Supp. No. 9, at 282, U.N. Doc. A/3159, (1956), *reprinted in* [1956] 2 Y.B. Int'l L. Comm'n 253, U.N. Doc. A/CN.4/SER.A/1956/Add.l.

[72] *Id.*

[73] UNCLOS, *supra* note 57, art. 100.

[74] *Id.* art. 101.

> same applies if the ship or aircraft has been used to commit any such act, so long as it *remains under the control* of the persons guilty of that act.[75]

The definition helps establish the rights and obligations of others in relation to the thing defined. Once a vessel is found to be "under the control" of "persons guilty of [piracy]" under UNCLOS Article 100, States have a right to arrest the pirates and try them in their domestic courts.[76]

The duty to cooperate in repressing piracy was further codified in 1988 when the International Maritime Organization, a U.N. agency, prepared the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention).[77] The SUA Convention imposed an affirmative obligation on States Parties to create criminal offenses in their municipal codes under which pirates could be prosecuted, and to either prosecute offenders found within their territories or extradite them to be prosecuted.[78] Most U.N. Member States have since acceded to the convention.[79]

While piracy itself is considered a *jus cogens* violation of international law,[80] an affirmative obligation on States to repress piracy exists only in treaties, making the duty to cooperate against pirates announced in Article 100 of UNCLOS and the SUA Convention an obligation *erga omnes partes*—owed by the parties to the Convention to each other—rather than an obligation *erga omnes*—an obligation on *all* States.[81] States that have been willing to accept these obligations in the SUA Convention with respect to piracy include many States with sophisticated cyber capabilities which could be used in

[75] *Id.* art. 103 (emphasis added).

[76] *See id.* arts. 100, 105.

[77] *See* Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 27 I.L.M. 672.

[78] *See* Fokas, *supra* note 61, at 440–41; Douglas Guilfoyle, *Piracy off Somalia: A Sketch of the Legal Framework*, EJIL:TALK! (Apr. 20, 2009), https://www.ejiltalk.org/piracy-off-somalia-a-sketch-of-the-legal-framework/ [https://perma.cc/CKW2-PFHJ].

[79] *See* INT'L MAR. ORG., STATUS OF IMO Treaties 442 (Sept. 10, 2021), https://www.cdn.imo.org/localresources/en/About/Conventions/StatusOfConventions/Status%20-%202021.pdf [https://perma.cc/Q2E5-HBQS].

[80] Int'l Law Comm'n, Fragmentation of International Law: Difficulties Arising from Diversification and Expansion of International Law, ¶ 374, U.N. Doc. A/CN.4/L.682 (2006).

[81] *But see* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, art. 48(1), U.N. Doc. A/56/10 (2001) (contemplating the possibility that an uninjured State could invoke the responsibility of another State if a breached obligation "is owed to the international community as a whole").

an analogous obligation to repress *cyber* pirates.[82] Offering the analogy raises the question as to whether these States would accept the same obligation to exercise jurisdiction over botnet operators if using a botnet was similarly defined in international law as a universally criminal "act of violence or detention . . . committed for private ends."[83]

B. *Case Study: U.N.-Authorized Multilateral Anti-Piracy Taskforce*

It is helpful to this analysis to observe how States have collectively operationalized international law regarding pirates, including their treaty obligations to cooperate in suppressing piracy. Since 2008, the U.N. Security Council has authorized operations conducted by a coalition of navies of U.N. Member States to counter pirates off the coast of Somalia.[84] These operations were originally conducted by the Combined Maritime Forces (CMF), a multinational coalition established in February 2002 by U.S. naval forces with a broader mission including anti-terrorism and anti-human trafficking efforts in the Red Sea, Arabian Sea, Indian Ocean, Gulf of Oman, and Gulf of Aden.[85] In 2009, the CMF created Combined Task Force (CTF) 151 specifically to "deter, disrupt and suppress piracy and armed robbery at sea."[86] Although membership in CTF 151 is "fluid," it typically consists of sailors and ships from about twenty-five States, and is currently under the rotating command of the Brazilian navy.[87]

The Security Council exercises the authority to identify threats and mandate responsive measures under Chapter VII of the U.N. Charter, which in Article 39 directs that the Council "shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken . . . to maintain or restore interna-

[82] These states include Estonia, Iran (a signatory), Russia, and the United Kingdom. *See* U.N. Treaty Collection, Chapter XXI(6), United Nations Convention on the Law of the Sea, https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en [https://perma.cc/U2CA-PJD6].

[83] UNCLOS, *supra* note 57, art. 101.

[84] *See* Ploch et al., *supra* note 43, at 19.

[85] *See* Lesley Anne Warner, *Pieces of Eight: An Appraisal of U.S. Counterpiracy Options in the Horn of Africa*, 63 Naval War Coll. Rev. 61, 72 (Spring 2010).

[86] *See CTF 151: Counter-Piracy*, Combined Maritime Forces, https://combinedmaritimeforces.com/ctf-151-counter-piracy/ [https://perma.cc/Z3NJ-VPCP]. "Armed robbery at sea" is distinguishable from piracy because it may refer to thefts within a State's territorial sea, where the State has exclusive jurisdiction, rather than on the high seas.

[87] *See* Ploch et al., *supra* note 43, at 25; *id.*

tional peace and security."[88] Under Article 41, the Security Council has broad discretion in deciding the measures needed "to give effect to its decisions" and in calling upon U.N. Member States "to apply such measures."[89] This power has been used, *inter alia*, to establish international criminal tribunals.[90]

In December 2020, the U.N. Security Council renewed authorization for States and multilateral organizations like CTF 151[91] to "use all necessary means to fight piracy off the coast" of Somalia.[92] In reauthorizing action against Somali pirates, the Security Council noted that "piracy exacerbates instability in Somalia by introducing large amounts of illicit cash that fuels additional crime, corruption, and terrorism."[93] The Security Council further urged States "to take appropriate actions under their existing domestic law, or develop legislative processes, to prevent the illicit financing of acts of piracy and the laundering of its proceeds."[94]

CTF 151 serves both a deterrent function and a law enforcement function.[95] As a deterrent, CTF 151-affiliated naval ships patrol waters, provide escort to merchant vessels, and, when confronting pirate vessels, confiscate their weapons and skiffs.[96] When pirates have hijacked vessels, CTF 151 member navies have attempted hostage rescues or even sunk the vessel.[97] In its international law

[88] U.N. Charter art. 39.

[89] U.N. Charter art. 41.

[90] *See* Prosecutor v. Tadiæ, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶¶ 31–35 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) ("Once the Security Council determines that a particular situation poses a threat to the peace . . . it enjoys a wide margin of discretion in choosing the course of action," which is not limited to the "illustrative examples" set out in U.N. Charter Articles 41-42.). *See also* LORI FISLER DAMROSCH & SEAN D. MURPHY, INTERNATIONAL LAW CASES AND MATERIALS 247-48 (7th ed. 2019) (asserting that the U.N. Security Council has taken a more proactive role in identifying threats to international peace and security with the rise of terrorism in the post-9/11 era).

[91] CTF 151 is not the only multilateral organization countering piracy in the Gulf of Aden; the European Union coordinates a task force and Egypt, Jordan, Qatar, and other states also formed an Arab Anti-Piracy Task Force in 2009. *See* James Warden, *Combined Task Force 151 Hunts Down Pirates in the Gulf of Aden*, STARS & STRIPES (Mar. 29, 2009), https://www.stripes.com/news/combined-task-force-151-hunts-down-pirates-in-the-gulf-of-aden-1.89695 [https://perma.cc/NF74-FVY4]; Warner, *supra* note 85, at 76.

[92] Press Release, Security Council, Security Council Renews Authorization for International Naval Forces Fighting Piracy Off Somali Coast, Unanimously Adopts Resolution 2554 (2020), U.N. Press Release SC/14373 (Dec. 4, 2020); *see also* S.C. Res. 2554, ¶ 12 (Dec. 4, 2020).

[93] S.C. Res. 2554, ¶ 2 (Dec. 4, 2020).

[94] *Id.* ¶ 17.

[95] *See* Guilfoyle, *supra* note 78.

[96] *See* Warner, *supra* note 85, at 72, 70.

[97] *See* Guilfoyle, *supra* note 78.

enforcement capacity, authorized by the U.N. Security Council, CTF 151 also captures pirates and brings them to countries that are able to prosecute them.[98] For instance, teams from the U.S. Naval Criminal Investigative Service have boarded vessels to collect and log evidence to preserve chain of custody for the purpose of aiding criminal prosecutions.[99] However, capturing pirates can raise legal dilemmas, such as ensuring that the length and manner of their detention conforms with international human rights law.[100] If the pirates harmed nationals from more than one State, there may be competing claims for jurisdiction.[101] Although universal jurisdiction can be exercised against pirates on the high seas, in the case of anti-piracy operations near Somalia, CTF 151's rare incursions into Somalian territory were premised on prior consent from Somalia.[102] Moreover, some States in the region cannot accept the pirates because their national courts lack the capacity or they do not have adequate criminal offenses in their municipal law.[103] In 2010, to augment successful piracy prosecutions in national courts in the Netherlands, United States, and Yemen, Kenya established a special court to try suspected pirates.[104]

Despite these challenges, naval patrols have had a strong deterrent effect. CTF 151 reports on its website that there has not been a successful piracy attack since 2017, and the last successful attack before that was five years prior.[105] Outside observers echo this report, crediting the naval presence in the Gulf of Aden with cutting the number of successful pirate attacks in half.[106] The Security Council acknowledged this success while reauthorizing CTF 151's efforts.[107]

Detractors of such an international cooperation success story may point out that States such as China and Russia do not participate, instead deploying ships to the region to monitor piracy and

[98] *See id.*

[99] *See* Warner, *supra* note 85, at 71, 73.

[100] *See id.* at 71.

[101] *See id.* at 70.

[102] *See* Guilfoyle, *supra* note 78; *see also* S.C. Res. 2554 at 1 (noting letter from Permanent Representative of Somalia to the United Nations "requesting international assistance to counter piracy off its coast").

[103] *See* Guilfoyle, *supra* note 78.

[104] *See* Dapo Akande, *Anti-Piracy Court Opens in Kenya*, EJIL:TALK! (June 28, 2010), https://www.ejiltalk.org/anti-piracy-court-opens-in-kenya/ [https://perma.cc/F7SE-4EAN].

[105] *See CTF 151: Counter-Piracy*, *supra* note 86.

[106] *See* Guilfoyle, *supra* note 78 (citing shipping industry estimates).

[107] *See* S.C. Res. 2554, para. 4 (Dec. 4, 2020).

escort ships flying their national flags independently of CTF 151.[108] But the U.N. Security Council specifically commended these States' parallel counter-piracy missions in the region and their efforts to deconflict their activities with those of CTF 151.[109] And China's engagement in multilateral policing might only just be starting; China's global footprint is expanding with its Belt and Road Initiative, and Beijing's willingness to spend resources to protect its assets abroad will likely grow with time.[110]

IV. Cyber Privateerism as a "Solution" to Cyber Piracy?

As evidenced by Microsoft's response to Trickbot, piracy also gives rise to privateers—those who use the tactics of pirates but do so under the sanction of a State.[111] While Microsoft did not receive a formal license from the U.S. Government to use cyber tools against Trickbot, its action was authorized by a U.S. court, which is an act attributable to the U.S. government under international law[112]—a practice comparable to prize courts identifying legally condemnable ships, as discussed below. What follows is a discussion of the historical authorization of privateers, the eventual renunciation of their use under international law, and the common problems privateers pose in both nautical and cyber settings.

A. *Historical Usage (and Denunciation) of Privateers*

Historically, privateers were private merchants authorized to capture enemy-flagged ships or enemy-owned goods on a neutral vessel by a State license known as a letter of marque, which "deputize[d] an individual or company."[113] This authority allowed privateers to seize enemy ships, bring their sailors back to port to be prosecuted, and receive compensation "much like a bounty

[108] *See* Ploch et al., *supra* note 43, at 25.

[109] *See* S.C. Res. 2554, para. 9 (Dec. 4, 2020).

[110] *See* Jimmy Zhang, Commentary, *From Non-Interference to Wolf Warrior: Chinese Foreign Internal Defense*, War on the Rocks (Apr. 24, 2020), https://warontherocks.com/2020/04/from-non-interference-to-wolf-warrior-chinese-foreign-internal-defense/ [https://perma.cc/3JR2-HYET].

[111] *See* George E. Burns, Jr., *The Legal War Against Mankind's Enemy*, 37 Md. B.J. 46, 46 (Sept./Oct. 2004).

[112] *See* Int'l Law Comm'n, *Articles on Responsibility of States for Internationally Wrongful Acts*, U.N. Doc. A/56/49, art. 4 (2001) ("The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions . . . .").

[113] Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, Army Law. 4, 5 (August 2013).

hunter."[114] Any enemy goods captured—including the enemy ship—would be sold at "[p]rize [c]ourts," with the State and the privateers typically splitting the earnings.[115] The prize courts were a formal judicial process; a privateer had to secure the judgment of a court that an enemy ship was "condemned" before it could be sold as a "lawful prize."[116] As one law professor has noted, "[a]ll eighteenth-century western European nations used privateers, but there nevertheless was a general agreement that privateers were not entirely trustworthy" because they had no military discipline and were motivated entirely by profit.[117]

Some have suggested that private actors should be similarly authorized by the United States to carry out cyber actions such as seizing and "digitally sequester[ing]" the laundered money of "rogue states"[118] or stealing back cryptocurrency that was stolen by hackers.[119] These commentators embrace the "profit motive" of these potential hackbackers, arguing that they should also be entitled to a share of the funds they retrieve in order to induce their participation.[120] One proponent of cyber letters of marque uses the nautical comparison and notes the success of privateers during the American Revolution: "American privateers devastated British commerce, funding the first two years of the war substantially through British captures."[121] But this belies a mismatch between the problem and this proffered solution: privateers historically were not used to solve the *collective* problem of piracy, but rather functioned as mercenaries on behalf of *individual* States.[122] Privateers "waged war for profit" instead of filling an ongoing law enforcement role.[123] Their "venture capitalist" incentive structure was not designed to induce long-term support of government enforcement measures.[124] Rather than an inherently positive attribute, privateers' "profit motive rendered them inherently *unreliable*

[114] *Id.*

[115] *Id.* at 11.

[116] *See* William R. Casto, *Regulating the New Privateers of the Twenty-First Century*, 37 Rutgers L.J. 671, 678–79 (2006).

[117] *Id.* at 678.

[118] Kessinger, *supra* note 113, at 10–11.

[119] *See* Joshua Parisi, *"WWW" Marques the Spot: Privateering as a Solution to Cryptocurrency Theft*, 72 SMU L. Rev. 895, 911–14 (2019) (recommending using Bitcoin as a "profit motive to incentivize private parties" as cyber privateers).

[120] *See id.* at 916–17 (noting that profit would be "necessary to incentivize those with the skills to act as cyber privateers").

[121] Kessinger, *supra* note 113, at 7.

[122] *See* Rosenzweig, *supra* note 37, at 112.

[123] Casto, *supra* note 116, at 680.

[124] *See id.* at 676.

for the accomplishment of missions that had no clear prospect of profit," as one scholar put it.[125]

Recognizing such disadvantages of privateers—and seeking to restrain their ubiquitous use in naval combat—55 States came to the conclusion in the mid-1800s that privateerism should be renounced just as piracy had been in order to "establish a uniform doctrine" that could resolve "differences of opinion" about which parties in naval conflicts were neutral and which were not.[126] The result was the Paris Declaration Respecting Maritime Law, signed in 1856, which reads in relevant part:

> 1. Privateering is, and remains, abolished;
> 2. The neutral flag covers enemy's goods, with the exception of contraband of war;
> 3. Neutral goods, with the exception of contraband of war, are not liable to capture under enemy's flag;
> 4. Blockades, in order to be binding, must be effective, that is to say, maintained by a force sufficient really to prevent access to the coast of the enemy.[127]

While the United States did not agree to the diplomatic policy expressed in the Declaration, U.S. President William McKinley announced that the United States would comply with it during the Spanish-American War, and the United States has not authorized any privateers since the Declaration was signed.[128]

Some States have issued letters of marque since the Declaration for the limited purposes of expressly authorizing self-defense and even permitting the capture of pirates.[129] However, merchants have traditionally been entitled to use self-defense under customary international law.[130] Some States' continued authorization of privateers speaks less to the general practice of States than it does to the Declaration's limits (it addressed use of privateers only in wartime) and to those States' flouting of customary international law. Under maritime law, "only state-owned vessels were given the privilege to board and seize a pirate ship or to engage in hot pur-

[125] *Id.* at 678 (emphasis added).

[126] Int'l Comm. of the Red Cross, Declaration Respecting Maritime Law (Apr. 16, 1856), https://ihl-databases.icrc.org/ihl/WebART/105%E2%80%9310001?OpenDocument [https://perma.cc/GQP8-WGLZ].

[127] *Id.*

[128] *See* Kessinger, *supra* note 113, at 9; *see also* Rosenzweig, *supra* note 37, at 113.

[129] *See* Rosenzweig, *supra* note 37, at 113. Professor Rosenzweig notes that the Transitional Federal Government of Somalia hired private contractors (essentially privateers) to help defend Somalia's coastline, *see id.* at n.40, but this occurred before the U.N. authorized the CMF's anti-piracy missions, which suggests that enlisting privateers failed to solve the piracy problem.

[130] *See id.* at 110.

suit of a pirate ship."[131] Article 107 of UNCLOS preserves this line of customary international law, making clear that only "warships . . . or other ships . . . clearly marked and identifiable as being on government service" are entitled to seize a ship on account of piracy.[132] Before the Declaration, one scholar has written, "privateering was typically permitted only during times of war."[133] Moreover, privateers were not given *carte blanche* on behalf of their private interests, but were enlisted to "aid the war effort by assisting in the destruction of the commerce of a hostile nation."[134]

B. *Cyber Privateers Pose the Same Problems as Privateers of Old*

In the cyber context, allowing a private company to use self-defense measures—such as beaconing and honeypots—parallels the Paris Declaration's demarcation of authorities, but permitting hot pursuit of a botnet raises a number of additional problems in common with their high seas counterparts. First, permitting privateers to take certain actions while prohibiting pirates from taking those same actions creates a paradoxical legal regime in which the same conduct is illegal for some but not others. Privateers are merely pirates who are beyond the reach of the law because they operate under the aegis of a State.[135] This dichotomy historically muddied the waters of pirate prosecutions, leading to "inexplicable arbitrariness" in some piracy trials.[136] One State's privateer could be another's pirate. Likewise, in cyberspace, going after cybercriminals can entail breaking privacy laws meant to constrain those same criminals.[137] As one commentator reflecting on piracy trials of the nineteenth century concluded, "[i]f the law is perceived simply as an arm of political policy, or as a means of revenge, it will fail to obtain the international credibility necessary to suppress international criminals."[138] Arguably, the law cannot credibly deter hackers if those same hackers can turn around and avoid prosecution by working as lawful privateers.

[131] *Id.*

[132] *See* UNCLOS, *supra* note 57, art. 107.

[133] Rosenzweig, *supra* note 37, at 112.

[134] *Id.*

[135] *See* Parisi, *supra* note 119, at 900; *see also* Casto, *supra* note 116, at 679 ("When Captain William Kidd sailed the Indian Ocean, he had a privateer's commission. Eventually, however, the British hanged him for exceeding his commission. Similarly, Blackbeard the pirate was at one time a British privateer.").

[136] Burns, *supra* note 111, at 49–50.

[137] *See generally* Shackelford et al., *supra* note 32 (assessing the anti-hacking statutes of China, Singapore, Thailand, Australia, and the members of the G7).

[138] Burns, *supra* note 111, at 50.

Perhaps the most damaging problem instigated by privateers is that their animating incentive is in continued conflict.[139] During the American Revolution, leaders of the fledgling Continental Navy struggled to recruit sailors because the prize money from a captured enemy ship was more lucrative than waiting for wages from a Continental Congress that did not always have the capital to pay its soldiers or sailors on time.[140] Residents of one seaport were even reported to be "dejected on the return of peace."[141] The same could be said today, when a talented coder can earn more money by pursuing hackers on behalf of a private cybersecurity company than as a member of CYBERCOM.[142] Allowing hackback could spawn an industry of cyber privateers whose profit is dependent on the continued existence of cyberthreats.[143] In such a milieu, when conflict ends, "privateers [are] unemployed and thus ha[ve] a strong incentive to become pirates."[144] Privateers are, after all, "rational wealth maximizers."[145]

Not only does cyber privateerism appear out of step with customary international law, but it also contradicts an "emerging international norm against [hackback]."[146] One comparative study of 20 States' laws found that many States restrict private actors from engaging in the kind of conduct considered hackback, with criminal penalties in the case of violation.[147] While some states have enlisted the help of private hackers, this has typically been in extreme situations. After Russia's 2022 invasion of Ukraine, for instance, reports suggested that Ukraine Defense Ministry officials made personal appeals to civilian hackers to help protect civilian infrastructure (though Ukrainian officials refused to publicly con-

[139] *See* EVAN THOMAS, JOHN PAUL JONES: SAILOR, HERO, FATHER OF THE AMERICAN NAVY 68–69 (2003); *see also* Burns, *supra* note 111, at 46.

[140] *See* THOMAS, *supra*, note 139, at 68–69.

[141] *Id.* at 68.

[142] *See* Josh Lospinoso, *Fish Out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It*, WAR ON THE ROCKS (July 12, 2018), https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/ [https://perma.cc/J7NG-HQR6].

[143] *See* Gerard, *supra* note 10, at 208 ("[T]he incentive model in private cybersecurity [does] not drive private cybersecurity firms to cure the problem—'to put themselves out of a job.'").

[144] Burns, *supra* note 111, at 46.

[145] *See* Casto, *supra* note 116, at 680.

[146] Shackelford et al., *supra* note 32, at 425.

[147] *See* Brian Corcoran, *A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace*, 11 HARV. NAT'L SEC. J. 1, 51 (2020) (noting that states tend to criminalize traditional "hackback" activities as defined in Section II.B of this note, including access to data at rest, modifying data at rest, intercepting data in transit, and hindering normal computer functions).

firm the request).[148] And, after suffering devastating cyberattacks in 2007, Estonia created a Cyber Defense League, a public-private partnership of cyber experts who could be called to service in the event of a future cyberattack.[149]

Even if not a general practice of States, there is "remarkable uniformity" in States' approaches to domestic criminal law regarding cyber activity, inching toward an international custom of opposing hackback.[150] Indeed, 78 states explicitly renounced hackback in the 2018 Paris Call for Trust and Stability in Cyberspace.[151] In March 2020, dozens of multinational companies launched the "Cybersecurity Tech Accord," which embraces this emerging custom.[152] In a post published to its website, the Accord recently affirmed its position against hackback, arguing that the principle of "'no private hack back' . . . is critical to a stable online world."

If hackback is not the answer, then the far more pressing discussion is one about how best to promote international cooperation against botnets, which may reasonably be called cyber pirates. Unlike the Paris Declaration, which renounced privateers, and the Security Council measures that established CTF 151, which provide for the pursuit of pirates off the coast of Somalia, there is no analogous agreement or rules to renounce hackback and pursue and repress botnets. Part V offers a cursory review of evolving military legal doctrine that may provide a part of the solution, followed, in Part VI, by a brief summarization of existing legal frameworks for global cooperation on cybercrime. Part VII concludes with a recommendation for a new international taskforce that can plug the gap these frameworks leave behind.

[148] Joel Schectman & Christopher Bing, *Ukraine Calls on Hacker Underground to Defend Against Russia*, Reuters (Feb. 24, 2022), https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ [https://perma.cc/J4F8-RMCU?type=image].

[149] Tom Gjelten, *Volunteer Cyber Army Emerges in Estonia*, NPR (Jan. 4, 2011), https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation [https://perma.cc/F3KP-XFF7].

[150] *Id.* at 2.

[151] *See* Section V.B, *infra.*

[152] *Advancing Cyber Hygiene and Speaking Out on Hack Backs: Recognizing the 2nd Anniversary of the Paris Call for Trust and Security in Cyberspace with Action*, Cybersecurity Tech Accord (Nov. 12, 2020), https://cybertechaccord.org/advancing-cyber-hygiene-and-speaking-out-on-hack-backs-recognizing-the-2nd-anniversary-of-the-paris-call-for-trust-and-security-in-cyberspace-with-action/ [https://perma.cc/3QWH-TCRA]. The 2018 Paris Call for Trust and Stability in Cyberspace, to which the post referred, is discussed more fully in Section VI.B. The number of private signatories has grown to 152 as of this writing.

V. Military Solutions to a Transnational Crime Problem?

It should not have escaped notice that the naval forces of several countries are presently tasked with suppressing what has long been considered criminal activity. In modern times, piracy has always been a subject of blended military–criminal enforcement action,[153] notwithstanding States' municipal anti-piracy laws, just as cyber conduct has blurred the boundaries between unlawful interference and outright use of force.

Determining whether a cyber action has risen to the level of a use of force unlawful under international law was the animating purpose behind the convening of the International Group of Experts (IGE), which produced the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn 2.0*), a non-legally-binding academic study of international law questions that arise in cyber intercourse between States.[154] Although it does not provide an answer to the present inquiry, *Tallinn 2.0* is a helpful reference that offers analogies and answers to parallel questions. For instance, *Tallinn 2.0* demonstrates that the obligation to repress piracy can theoretically extend to repressing *cyber* means of *conducting* piracy.[155] *Tallinn 2.0* observes that, because Article 110 of UNCLOS permits warships the authority to board foreign vessels when there is a "reasonable ground for suspecting" that the vessel is engaged in piracy, a State vessel could be justified in boarding a foreign vessel if there were evidence that those on board the latter were using cyber means to facilitate an act of piracy (e.g., communicating to pirates on another vessel via social media).[156] But, given that the definition of piracy depends on acts committed on the high seas, defeating botnets is not as simple as declaring them pirates under international law.

Of course, military forces have increasingly been used to solve problems of transnational crime. As Professor Dan Stigall has written, international law "tightly constrains . . . extraterritorial civilian law enforcement operations while granting the military (in certain

[153] *See supra* text accompanying notes 65–67. Piracy has been analyzed under the law of war, and "piratical" acts were understood in the Lieber Code, an early codification of the law of war conducted by the U.S. Army, to be "war crimes" where the law of war applied. Rubin, *supra* note 59, at 293.

[154] *See* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 1-3 (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017) [hereinafter Tallinn 2.0]. For the IGE's (International Group of Experts) conclusions on this question, *see, e.g.*, *id.* at 330–333 (providing academic conclusions on the definition of use of force).

[155] *See id.* at 235–36.

[156] *See id.* at 235–36.

circumstances) wide latitude."[157] The result is "the increasingly common" use of one State's military forces in another "to reestablish a safe and secure environment and provide essential government services" alongside local authorities—missions referred to as "stability operations."[158] It is thus not hard to imagine one State welcoming the cyber forces of another to "perform[ ] civilian police functions" like investigating cybercrimes and arresting botnet controllers, approximating the "stability operations" carried out by U.S. forces in Iraq.[159]

Additionally, although such a discussion is beyond the scope of this Note, it is worth pausing to consider how force against non-state cyber threats such as botnets may be justified. In justifying U.S. military operations against the Islamic State of Iraq and the Levant (ISIL), for instance, Brian Egan, the U.S. State Department Legal Adviser in 2016, noted that States have historically invoked the "inherent right" of self-defense against non-State actors.[160] Like jurisdictional questions, use of force on another State's territory—even in self-defense—must account for a State's sovereignty.[161] As with enforcement jurisdiction, which may be exercised in another State with that State's consent, use of force in self-defense against a non-State actor taking refuge in another State respects State sovereignty where the defending State has obtained the territorial State's consent. The legal rationale underpinning U.S. airstrikes against ISIL in Syrian territory, however, rested not on Syria's consent but on an "unable or unwilling" standard: where a State relies on self-defense to use force against a non-State actor on another State's territory and does not have the territorial State's consent, it must "determine that the territorial State is 'unable or unwilling' to address the threat posed by the non-State actor on its territory."[162]

Such a legal rationale could theoretically be transposed to the cyber domain in a State which lacks the resources to dismantle botnets on its territory. However, it is based in the law of self-defense, and would therefore require a legal finding that a botnet's action rose to the level of an armed attack justifying use of force

[157] Stigall, *supra* note 55, at 5.

[158] *Id.* at 39 (internal quotation marks and citation omitted).

[159] *See id.* at 39–41.

[160] *See* Brian Egan, Legal Adviser, U.S. Dep't of State, Keynote Address at the 110th Annual Meeting of the American Society of International Law (Apr. 1, 2016), https://2009-2017.state.gov/s/l/releases/remarks/255493.htm [https://perma.cc/D42R-AJSZ].

[161] *See id.*

[162] *See id.*

(i.e., dismantling the offending botnet) in self-defense.[163] Under customary international law, only the *victim* of such an armed attack would be justified in using self-defense, or in requesting the help of others to initiate collective self-defense.[164]

VI. Existing International Cooperation Against Cybercrime

Two parallel U.N. working groups are actively negotiating in efforts to build consensus on responsible State behavior in cyberspace and the application of existing bodies of international law to States' cyber actions.[165] In May 2021, one of these groups[166] released an advance copy of its report, in which its 25 members—including the five Permanent Members of the Security Council—ostensibly agreed to a series of non-binding "norms" of State behavior in cyberspace. These norms included "not knowingly allow[ing] their territory to be used for internationally wrongful acts" in cyberspace and cooperating in prosecuting criminal use of information and communication technologies (ICT).[167] Of note, the report also suggests that "States may need to consider whether new measures need to be developed" to enable States to cooperate.[168] However, as States continue to negotiate these non-binding "norms," this Part surveys those agreements between States which already exist and are to some extent enforceable.

[163] *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense *if an armed attack occurs* against a Member of the United Nations . . . .") (emphasis added); *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 ¶¶ 229-36 (June 27) (discussing whether actions claimed by United States as justification for exercise of self-defense in fact constituted "armed attack" as the United States claimed).

[164] *See* Nicar. v. U.S., 1986 I.C.J. ¶¶ 195, 199.

[165] *See* Adina Ponta, *Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes*, 25 Am. Soc'y Int'l L.: Insights, no. 14 (July 30, 2021), https://www.asil.org/insights/volume/25/issue/14 [https://perma.cc/63QM-92LU].

[166] The Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security was established by the U.N. Secretary General pursuant to a U.S.-sponsored General Assembly resolution. *See generally* G.A. Res. 73/266 (Jan. 2, 2019).

[167] Report of the Group of Government Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Advance Copy at 6–7 (May 28, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf [https://perma.cc/H9RD-6CMK].

[168] *Id.* at 7.

A. *The Budapest Convention: Coordinating Laws but not Operations Against Botnets*

The Council of Europe Convention on Cybercrime (also known as the "Budapest Convention") was an early effort at standardizing countries' laws against Internet-enabled crimes.[169] However, its application here is limited because the Budapest Convention is inward-looking rather than oriented toward collective solutions. Like the SUA Convention, it identifies model legislation that the States Parties agreed to implement in their individual jurisdictions, such as making accessing a computer without authorization[170] or to infringing copyright "by means of a computer system"[171] into criminal offenses. The model criminal statutes identified by the Budapest Convention even include the conduct required to form a botnet, which includes illegal access to others' computer systems, interception of others' data, and interference with their systems.[172] But, while the Budapest Convention establishes "[g]eneral principles relating to international co-operation [and] mutual assistance,[173] it creates no enforcement mechanism or governing body to coordinate mutual assistance, instead leaving it to the States Parties to request help from each other when needed.[174]

Although it establishes a baseline procedural framework for promoting information-sharing and mandating mutual assistance,[175] the Budapest Convention reinforces the jurisdictional boundaries that complicate the fight against botnets. Yet, "as botnets have become larger and more overtly transnational in scope and

[169] *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, https://rm.coe.int/1680081561 [https://perma.cc/PVL6-VDMF] [hereinafter Budapest Convention].

[170] *See id.* ch. 2, § 1, art. 2.

[171] *Id.* ch. 2, § 1, art. 10.

[172] *See, e.g.*, Cybercrime Convention Comm., Council of Eur., T-CY Guidance Note #2: Provisions of the Budapest Convention Covering Botnets at 4, T-CY 6E Rev. (2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 [https://perma.cc/V8US-D3LF] [hereinafter Provisions of the Budapest Convention Covering Botnets].

[173] *See* Budapest Convention, ch. 3, § 1, arts. 23–25.

[174] Article 31 requires that, where a signing party requests help from another in accessing or seizing data, "[t]he requested Party *shall* respond to the request." *See id.* ch. 3, § 2, tit. 2, art. 31 (emphasis added). While Article 35 requires signing parties to designate a point of contact available on a 24-hour, 7-day-a-week basis for handling such requests. *Id.* art. 35. But the articles do not suggest which requests should be prioritized, nor does the Budapest Convention create a central body to coordinate the member states' efforts or identify common cyber threats.

[175] *See* Gerard, *supra* note 10, at 225.

effect,"[176] harmonization of domestic criminal law may not be the most effective response. Botnets pose the same jurisdictional challenges that pirates once did in that they operate on the international plane, outside the jurisdiction of any one State, and do so anonymously.[177] Indeed, as one author made clear, the question of "whose jurisdiction should predominate" over malware autonomously sent from one computer to another, across a State border, by a botnet controller "whose home jurisdiction is hidden by data-anonymizing software" is not a simple question to answer.[178]

B. *The Paris Call's Attempt to Create a "Norm" Against Hackback*

The 2018 Paris Call for Trust and Stability in Cyberspace (Paris Call), a non-legally-binding statement signed by 81 states, "reaffirmed" that "customary international law is applicable to the use of [ICT] by States."[179] The Paris Call is silent on what aspects of customary international law may have the most salient application in cyberspace. However, the Paris Call does reflect the opinions of the 81 States that have signed it.

Notably, the Paris Call announces the opinion of its signatories that the United Nations is the proper forum for developing capacity-building measures.[180] It calls for Member States to "develop ways to prevent the proliferation of malicious [cyber] tools" (Principle 5) and also explicitly renounces hackback by private actors (Principle 8).[181] Although these principles may contribute over time to the general practice of states and *opinio juris*, and thus to customary international law,[182] none of them are currently binding on States because the Paris Call was not concluded as a treaty.

Although the Paris Call may be an early sign of growing consensus among States that hackback should be prohibited, the fact that three of the States most active in proposing international rules regarding State behavior in cyberspace—China, Russia, and the United States—have not signed on to it also leaves the prospect of

[176] *Id.* at 215.

[177] See discussion comparing botnets to pirates in Section II.C, *supra.*

[178] *See* Gerard, *supra* note 10, at 216.

[179] Paris Call for Trust and Stability in Cyberspace, para. 3, *opened for signature* Nov. 12, 2018, https://pariscall.international/en/call [https://perma.cc/G2SW-R85A] [hereinafter Paris Call for Trust and Security in Cyberspace].

[180] *Id.*, para. 5.

[181] *Id.*, para. 18; *see also The 9 Principles*, PARIS CALL, https://pariscall.international/en/principles [https://perma.cc/Y6W6-SWUM].

[182] *See* Int'l Law Comm'n, *supra* note 70, at 132 ("Conclusion 5: State practice consists of conduct of the State, whether in the exercise of its executive, legislative, judicial or other functions.").

future consensus in doubt. Moreover, the fact that U.S. courts have essentially sanctioned hackback, albeit in limited circumstances,[183] and that Ukraine has potentially enlisted civilian hackers in its 2022 armed conflict with Russia,[184] could portend the development of an alternative State practice.

C. *Case Study: Joint Cybercrime Action Taskforce as a Potential Model for Action Against Botnets*

There is at least one multistate group coordinating efforts to fight cybercrime: the Joint Cybercrime Action Taskforce (J-CAT), launched in September 2014 by the European Union Agency for Law Enforcement Cooperation (Europol).[185] J-CAT is comprised of a "standing operational team of cyber liaison officers" from nine European Union (EU) Member States, Europol's cybercrime unit known as the European Cybercrime Centre (EC3), and seven non-EU partner countries, including the United States, which is represented on J-CAT by the Federal Bureau of Investigation (FBI) and the Secret Service.[186]

J-CAT chooses which cases to pursue based in part on proposals from the country liaison officers.[187] Its work has largely focused on law enforcement actions, such as arresting those responsible for transnational payment fraud and online child sexual exploitation.[188] But J-CAT has had at least one major success against a botnet: in 2017, a joint operation of J-CAT, FBI, German law enforcement, and the EU Agency for Criminal Justice Cooperation dismantled the Andromeda botnet, which had coopted at least one million machines every month.[189] The botnet was used to distribute malware via links sent to other machines through social

[183] *See* Microsoft v. John Does 1–2, No. 1:20-cv-1171 (AJT/IDD) (E.D. Va. Oct. 20, 2020) (order granting preliminary injunction); *see also* Gerard, *supra* note 10, at 206 (describing two other cases in which Federal district courts allowed Microsoft to go on the offensive against alleged hackers).

[184] *See* discussion at Section III.B *supra*.

[185] *See Joint Cybercrime Action Taskforce (J-CAT)*, Europol, https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce [https://perma.cc/5GHU-D3J4].

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *See* Press Release, Europol, Andromeda Botnet Dismantled in International Cyber Operation (Dec. 4, 2017), https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation [https://perma.cc/P32F-5UWA].

media, instant messaging, and other means.[190] Andromeda itself demonstrates why coordinated multi-jurisdictional groups are necessary to dismantle botnets: Andromeda lasted for six years, surviving by updating its malware five times and by combining what were actually 464 distinct botnets and "1,214 domains and IP addresses of the botnet's command-and-control servers."[191]

Despite these successes, J-CAT is a small organization. From its inception in 2014, when it completed three operations, it only grew to complete 18 operations in 2019.[192] Its membership and the fact that it is housed under Europol auspices also give J-CAT a regional, rather than global, focus. Like their non-involvement in CTF 151, Russia's and China's absence from J-CAT is conspicuous.

D. *Do Competing Legal Theories Blockade Cooperation in Cyberspace?*

Of course, the discussion of international cooperation to dismantle botnets is complicated by the fact that botnets are not entirely separate from State action any more than high seas privateers once were. Investigators discovered that the creator of the GameOver Zeus botnet used its zombie computers to search for items that would be useful to Russian intelligence—email addresses of Georgian intelligence officers and classified Ukrainian government information, for example—even though they could not find a direct link to Russian intelligence.[193] GameOver Zeus even "redirected a section of [the] botnet to search for politically sensitive information on infected Ukrainian computers" during Russia's operation to seize Crimea.[194] Meanwhile, some cyber researchers have attributed the Ryuk ransomware—which activates in computers after they are infected by Trickbot—to North Korea because of its similarities to another type of ransomware that has

[190] *See* Ionut Arghire, *Andromeda Botnet to Die Slow, Painful Death*, SECURITYWEEK (Jan. 4, 2018), https://www.securityweek.com/andromeda-botnet-die-slow-painful-death-after-takedown [https://perma.cc/X7GD-FKDU].

[191] *Id.*

[192] *See Joint Cybercrime Action Taskforce (J-CAT)*, *supra* note 185.

[193] *See* Garett Graff, *Inside the Hunt for Russia's Most Notorious Hacker*, WIRED (Mar. 21, 2017), https://www.wired.com/2017/03/russian-hacker-spy-botnet/ [https://perma.cc/BTQ5-A6HP]. Russia has been known to offer safe harbor to cybercriminals in its territory as long as they do not attack Russian targets. Joseph Marks & Aaron Schaffer, *The Cybersecurity 202: Russia's the Capital of Ransomware, but It's Not the Only Player*, WASH. POST (July 20, 2021), https://www.washingtonpost.com/politics/2021/07/21/cybersecurity-202-russias-capital-ransomware-its-not-only-player/ [https://perma.cc/VT4N-QHHU]; *see also* ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS 11 n.* (2019) (noting that Russia is "known to look the other way" when cybercrime is focused on Western victims).

[194] Graff, *supra* note 193.

been attributed to North Korean government hackers.[195] The U.S. Department of Justice has also alleged that the North Korean government conspired with its citizen-hackers to spread malware through the Joanap botnet.[196]

Despite its potential connection to a criminal botnet, Russia spearheaded the passage of U.N. General Assembly Resolution 73/27 (G.A. Res. 73/27), which calls on States to, among other things, cooperate on prosecuting cybercrime and "prevent the proliferation of malicious [ICT] tools and techniques."[197] G.A. Res. 73/27 also called for the establishment of the second of the two "parallel" working groups referenced above, the Open-Ended Working Group, which published its own Final Substantive Report in March 2021.[198]

China has also been actively developing its own philosophy of cyber "norms" on the world stage through its leadership of the Shanghai Cooperation Organization (SCO).[199] In 2015, the SCO submitted to the U.N. Secretary-General a proposed "International Code of Conduct for Information Security" (Code of Conduct) and invited States to sign on.[200] Like G.A. Res. 73/27, the proposed Code of Conduct also highlights "the need for enhanced . . .

[195] *See* Kimberly Goody et al., *A Nasty Trick: From Credential Theft Malware to Business Disruption*, FireEye Threat Rsch. Blog (Jan. 11, 2019), https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html [https://perma.cc/W8WU-RP5X].

[196] Complaint at 3, United States v. Hyok, No. 18-mj-1479 (C.D. Cal. June 8, 2018); *see also* Sean Lyngaas, *U.S. Announces Disruption of 'Joanap' Botnet Linked with North Korea*, CyberScoop (Jan. 30, 2019), https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/ [https://perma.cc/VL6G-HEBY] (discussing the Department of Justice's complaint).

[197] G.A. Res. 73/27, ¶¶ 1.4, 1.10 (Dec. 11, 2018); *see also* Veni Markovski & Alexey Trepykhalin, ICANN, Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations 7 (Jan. 19, 2021), https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-006-19jan21-en.pdf [https://perma.cc/Z5KL-CY4F] (discussing President Putin's statement on Russia-United States cooperation in the area of information security).

[198] Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Rep., ¶ 6, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021).

[199] *See Shanghai Cooperation Organization*, U.N. Dep't Pol. & Peacebuilding Affs. https://dppa.un.org/en/shanghai-cooperation-organization [https://dppa.un.org/en/shanghai-cooperation-organization].

[200] *See* Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the U.N., Letter dated Jan. 9, 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 22, 2015) [hereinafter Proposed Code of Conduct]. The 2015 document is a revised version of a 2011 letter; *see* U.N. Doc. A/66/359 (Sept. 14, 2011).

cooperation among States in combating the criminal misuse of information technologies."[201] In addition, the Code of Conduct suggests the need to use information and communication technologies in accordance with "maintaining international peace and security."[202] To Western ears, the Code of Conduct's more controversial provisions include its affirmation that "policy authority for Internet-related public issues is the sovereign right of States."[203]

The Code of Conduct embodies China's "cyber sovereignty" model of Internet governance, a position Russia largely shares, which is premised on the argument that States should have control over the Internet within their borders without outside interference.[204] While the "cyber sovereignty" model seems primarily concerned with blocking attempts to circumvent Internet censorship,[205] it is likely incompatible with international cooperation on cybercrime generally, or more specifically, on attacking common online threats like botnets. China, like Russia, may be cooperating with criminal gangs to deflect cyberattacks away from its own citizens: In July 2021, the United States and several of its allies attributed a significant breach of Microsoft to hackers "affiliated with" China's Ministry of State Security.[206]

The Sino-Russian "cyber sovereignty" model is often framed as the chief competitor to an "open, interoperable" U.S.-led model.[207] Allison Peters, previously at the think tank Third Way and now a Senior Advisor at the U.S. State Department, has described the U.S. model as a Budapest Convention-aligned system based on cooperating against cybercrime and keeping the Internet essen-

[201] Proposed Code of Conduct, *supra* note 200, at 3.

[202] *See id.* at 5.

[203] *Id.* at 3.

[204] *See* Valentin Weber, *The Sinicization of Russia's Cyber Sovereignty Model*, COUNCIL ON FOREIGN REL. BLOG (Apr. 1, 2020), https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model [https://perma.cc/Y2HB-L7PL].

[205] *See id.*

[206] Press Release, The White House, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ [https://perma.cc/5CU9-WM7W]; *see also* Marks, *supra* note 193 (stating that the White House statement accused the Ministry of State Security of "contracting with criminal gangs for some of its hacking work").

[207] "Cyber sovereignty" appears contrary to the 2018 U.S. Cyber Strategy, which included as priorities the protection and promotion of freedom of expression online. *See* THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 1-2 (Sept. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/6QES-6KSM].

tially borderless and censor-free.[208] Indeed, despite their calls for international cooperation against cybercrime, neither China nor Russia are party to the Budapest Convention, and the SCO is not an observer organization to the Convention.[209] Peters suggests that Russia's and China's refusals to join the Budapest Convention and their calls for a new cybercrime treaty are designed to start negotiations about rules of State behavior in cyberspace from scratch at the United Nations, where these two States wield influence as Permanent Members of the Security Council.[210] But, notably, the Open-Ended Working Group, created by a U.N. General Assembly Resolution; the Code of Conduct, submitted to the U.N. Secretary-General; and the Paris Call, signed by many of the parties to the Budapest Convention all agree that the United Nations is the right forum for the development of these rules.[211] U.S. allies France and Germany have also embraced theories of sovereignty in cyberspace, though this conflicts with their recent cooperation in botnet takedowns which likely violated state sovereignty, according to France's own definition.[212]

Finally, one author has suggested that, rather than a framework for coordinating action, the long-term solution to botnets may establish itself as a duty of States to mitigate cyber threats emanating from one's own territory.[213] Rhetorically, this argument has found favor with political leaders. In their first bilateral meeting, U.S. President Joe Biden reportedly told Russian President Vladimir Putin that "[r]esponsible countries need to take action against

[208] *See, e.g.*, Allison Peters, Argument, *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime*, FOREIGN POL'Y (Sept. 16, 2019), https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/ [https://perma.cc/6T3F-WHKR].

[209] Russia has observer status as a member state of the Council of Europe. *See Parties/ Observers to the Budapest Convention and Observer Organisations to the T-CY*, COUNCIL OF EUR. (Mar. 7, 2021), https://www.coe.int/en/web/cybercrime/parties-observers [https://perma.cc/Q2NA-MCRS].

[210] *See* Peters, *supra* note 208.

[211] *See* Paris Call for Trust and Stability in Cyberspace, *supra* note 179, para. 5; *see also* Proposed Code of Conduct, *supra* note 200, at 6.

[212] *See* Jack Kenny, *France, Cyber Operations and Sovereignty: The 'Purist' Approach to Sovereignty and Contradictory State Practice*, LAWFARE (Mar. 12, 2021), https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice [https://perma.cc/HA5C-2CYA] (explaining that the French Ministry of Armed Forces considers a cyber operation that produces any effects on French territory to violate French sovereignty).

[213] *See* Gerard, *supra* note 10, at 229.

criminals who conduct ransomware activities on their territory."[214] However, the "trend" in international law, as two law professors put it, "has been to move away from these general, abstract and vague notions, and instead to define the specific conduct expected by states to prevent harm to other states."[215] In the military context, a minority of the IGE which produced *Tallinn 2.0* supported the view that "affording sanctuary . . . to those mounting cyber operations . . . amounts to a 'use of force'" justifying self-defense measures.[216] Moreover, finding a duty in international law to end such sanctuary still would not account for when a State lacks the resources to comply with that duty.

Defining the conduct which States should be responsible for repressing is the very goal of this analysis. In the Part that follows, this Note argues that formal international cooperation against botnets, endorsed by the United Nations, is precisely what is needed—not only to defeat botnets themselves, but to influence the development of customary international law in cyberspace toward de-escalation and deconfliction through international cooperation on a common problem.

VII. Defining the Solution: Authorizing Action Against Botnets

The methods for defeating botnets are not a mystery. Information about which Internet Service Providers and IP Addresses are the "originators or relay points" can be shared with those providers, who can then disconnect the malware-spreading computers from their service to allow for mitigation.[217] Indeed, in granting Microsoft's request to disconnect Trickbot's "zombie" computers from the Internet so they could no longer serve the botnet, the U.S. District Court ordered Internet Service Providers to, *inter alia*, identify the Internet traffic originating from the suspect IP Addresses and "[t]ake reasonable steps to block [that traffic]," as well as "disable the computers . . . associated with the IP Addresses."[218] Typically, a botnet is defeated by redirecting the zombie computers' communications with the command-and-con-

[214] Martin Matishak, *Biden Says He Told Putin U.S. Will Hack Back Against Future Russian Cyberattacks*, Politico (June 16, 2021, 2:59 PM), https://www.politico.com/news/2021/06/16/biden-putin-russia-cyberattacks-494888.

[215] *See* Damrosch & Murphy, *supra* note 90, at 495.

[216] Tallinn 2.0, *supra* note 154, at 332.

[217] *See* Singer & Friedman, *supra* note 8, at 176.

[218] Microsoft Corporation v. John Does 1-2, No. 1:20-cv-1171 (AJT/IDD), at 9 (E.D. Va. Oct. 20, 2020) (order granting preliminary injunction).

trol server into a dummy server referred to as a "sinkhole," which receives the zombie computers' signals but sends no instructions back.[219] In addition, owners of infected computers need to be notified, and infected servers—often located in various States—need to be seized and dismantled so that they cannot be used to resurrect the botnet. Usually, court orders must be obtained to seize the servers in the different jurisdictions.[220] Naturally, this requires a tremendous amount of cross-border and public-private coordination.[221]

Thus, what is needed to defeat the growing number of botnets is not the expertise in taking them offline, but rather, a steady number of researchers, lawyers, and coders working together—and a central authority that can authorize such a law enforcement team to follow a botnet's virtual trail, even if it leads across national borders. On one hand is the question of what can be done against botnets *now*. On the other is the question of how the law may develop, through the practice of States in conjunction with what they view as their legal responsibilities, to dictate States' behavior in cyberspace. In answer to the first question, one potential solution is an addendum to the Budapest Convention which would give States Parties broader authorities to pursue and sinkhole command-and-control servers in each other's territories.[222] Another, more dramatic, step investigated here is the concept of an international taskforce modeled after CTF 151.

J-CAT comes closest to the kind of taskforce to defeat botnets envisioned here. But J-CAT has a running list of priorities. A proposal to defeat a botnet has to compete for resources with J-CAT's other projects, like pursuing those propagating child exploitation material or engaging in cross-border payment fraud schemes.[223] J-CAT is also limited by its regional scope and, given the coordination with local jurisdictions currently necessary to dismantle botnets, is logically limited to States which have model cybercrime offenses written into their municipal law—generally Budapest Con-

[219] *See* Graff, *supra* note 193; *see also* Harrington, *supra* note 34, at 17 (elaborating on the concept of sinkholing).

[220] Telephone interview with Luke Dembosky, Partner, Debevoise & Plimpton, and former U.S. Deputy Assistant Attorney General for National Security (Feb. 26, 2021) (memorandum on file with *The George Washington International Law Review*) [hereinafter Dembosky Interview].

[221] *Id.*

[222] Updates to the Budapest Convention seem to be one solution to the problems posed by botnets contemplated by Gerard, *supra* note 10, at 224–27.

[223] *See* discussion of J-CAT in Section VI.C, *supra*.

vention parties.[224] The need for something more than J-CAT is not a criticism of its efforts, but an acknowledgment that the problem is endemic and requires a global response that is beyond both the capacity of J-CAT and its regional scope.

CTF 151's missions against pirates off the coast of Somalia, authorized by the U.N. Security Council, offer a model for how a joint taskforce like J-CAT could be operationalized against the threat of botnets. One of the strengths of CTF 151's mandate is that it is authorized by the U.N. Security Council,[225] and an analogous anti-botnet taskforce should be similarly authorized. The 81 signatories to the Paris Call agree that the United Nations is the proper forum for such "confidence and capacity-building measures."[226] Given the U.N. Security Council's authority under Article 39 of the U.N. Charter—and its growing willingness to use that authority in the post-9/11 era[227]—U.N. Security Council authorization is the most effective and consensus-building place to start. Even those States that have not joined CTF 151 and its rotating command—namely, China and Russia—run parallel anti-piracy operations that actively cooperate with the U.N.-sanctioned CTF 151.[228] Their cooperation has led to successful deconfliction in multinational anti-piracy operations. As discussed in greater detail in Part VII.C *infra*, similar deconfliction in cyberspace could lead to common "rules of the road" and, eventually, to better attribution, which can deter confrontational State conduct in cyberspace over time.

A. *U.N. Security Council Authorization and a Three-Part Framework for Confronting Botnets*

Under its Article 39 authority, the U.N. Security Council should declare botnets a "threat to the peace" and authorize a joint botnet action taskforce (J-BAT) to dismantle botnets as a measure to "restore international peace and security."[229] Logistically, J-BAT could be housed under the auspices of J-CAT, and anyone at J-CAT currently working on an ongoing botnet disruption operation could migrate to J-BAT permanently to work on anti-botnet operations. States with the resources to take part should lend some of

[224] *See* discussion in Section VI.C *supra.*

[225] *See* S.C. Res. 2554, at 2 (Dec. 4, 2020).

[226] *See* Paris Call for Trust and Stability in Cyberspace, *supra* note 179.

[227] *See* DAMROSCH & MURPHY, *supra* note 90.

[228] *See* discussion in Section III.A *supra.*

[229] U.N. Charter, art. 39.

their best cyber investigators to the team. A rotating command, like that of CTF 151,[230] could ensure that the team targets botnets around the world, not just those preying on certain States' economies. For those States with less sophisticated cybercrime teams, a joint taskforce would foster the sharing of best practices, which those States could bring home to aid their domestic cybercrime prosecutions. Because of the interconnected nature of the Internet, the implementation of best practices in one State will help to make the Internet safer for all.[231]

Legally, a U.N. Security Council resolution authorizing J-BAT would solve some of the similar jurisdictional challenges to prosecution that other Security Council resolutions helped alleviate in the context of counter-piracy operations. CTF 151 is empowered to detain pirates and bring them to jurisdictions able to prosecute them. J-BAT could be empowered to "sinkhole" botnets. In order to implement the measures identified by the Security Council, Member States may find that they have an obligation to compel Internet Service Providers to cooperate in redirecting botnet traffic.[232] Although pirates are subject to universal jurisdiction,[233] such a legal tool would not necessarily be needed to redirect Internet traffic, which is vastly different from detaining the responsible suspect.

Arrest and prosecution of botnet controllers would be the second step in botnet "takedowns"—but need not even be executed by J-BAT, which could simply share the evidence it gathered with competent national authorities. The Budapest Convention, while not providing a fully sufficient organizing regime for J-BAT, does aid in prosecuting botnet controllers once J-BAT discovers them. The Budapest Convention requires States Parties to codify in their municipal law the kind of cyber-enabled crimes used to create botnets;[234] these States could therefore accept the operators of botnets for prosecution. While they may not want to accept botnet

[230] *See* discussion of CTF 151 in Section III.B *supra.*

[231] The sharing of best practices is widely viewed as a necessary element in defeating cyber threats. *See, e.g.*, *Joint Cybercrime Action Taskforce (J-CAT)*, *supra* note 185; Proposed Code of Conduct, *supra* note 200, at 6.

[232] The IGE which produced *Tallinn 2.0* similarly postulated that, should the Security Council identify a cyber operation as a "threat to the peace" pursuant to Art. 39 of the U.N. Charter and take measures pursuant to Art. 41, Member States would have an obligation according to Art. 25 to "carry out" the Security Council's "decisions." *See* TALLINN 2.0, *supra* note 154, at 357–58.

[233] *See* Wilson, *supra* note 61.

[234] *See* PROVISIONS OF THE BUDAPEST CONVENTION COVERING BOTNETS, *supra* note 172, at 4.

operators because their courts lack capacity to prosecute them, they would not have to turn them away for want of national laws enabling prosecution, as is the case with some States unable to accept pirates captured by CTF 151.[235] In this way, a Security Council resolution requiring States to cooperate toward the end of dismantling botnets could have the effect of enforcing the Budapest Convention. If capacity to prosecute botnet operators proves to be a problem, the international community may consider funding a special court, like the special piracy court in Kenya,[236] but such a need is not contemplated by this Note and has not yet been discovered in the literature.

The Security Council may consider the more provocative step of empowering J-BAT physically to dismantle the infrastructure of botnets in States that do not have the capacity to do so themselves. Seizure of botnet infrastructure and suspect controllers is occasionally undertaken by members of J-CAT, but in close coordination with local authorities.[237] Imposing on Member States the obligation to permit J-BAT officers into their territories to seize servers used to create a botnet—perhaps under a theory of universal jurisdiction over cybercriminals—would be quite different. However, such an operation is not wholly unprecedented, but rather, might evoke "stability operations" such as those performed by U.S. forces in Iraq to support local law enforcement.[238] States struggling to contain cybercrime may welcome the logistical support and training; then, of course, the operation would be based on territorial State consent rather than the "unable or unwilling" standard espoused in the military intervention context.[239] In the growing number of States passing such laws,[240] J-BAT officers could merely enforce municipal law, reinforcing the capacity of local authorities. A Security Council Resolution encouraging such consent-based capacity-building operations would do much to advance the global

[235] *See* discussion in Section III.B *supra.*

[236] *See id.*

[237] Europol has also coordinated with the local authorities of multiple states to arrest criminals using the dark web. *See, e.g.*, *150 Arrested in Dark Web Drug Bust as Police Seize _26 Million*, EUROPOL (Oct. 26, 2021), https://www.europol.europa.eu/media-press/newsroom/news/150-arrested-in-dark-web-drug-bust-police-seize-_26-million [https://perma.cc/R8FG-4LCZ].

[238] *See* Stigall, *supra* note 55, at 39–42.

[239] *See* Egan, *supra* note 160.

[240] *See generally* Corcoran, *supra* note 147 (surveying twenty states' cybercrime laws and concluding that they are evidence of an emerging state practice to criminalize certain activities).

fight against botnets, and alleviate distrust of such cross-border operations.

Even failing the ability to capture botnet controllers, or to obtain court orders to seize their server infrastructure, J-BAT would serve a significant deterrent function just as CTF 151 does with its patrols. The more widely known J-BAT becomes, the more aware potential botnet controllers will be that an international team is working to shut down their operations. If botnet controllers adapt their behavior to avoid prosecution by fleeing to States where they cannot be prosecuted, they will only contribute to increasing international pressure on those States to comply with a developing custom of States to prosecute botnet controllers.

J-BAT's enforcement and deterrence functions are best illustrated by considering three general categories of botnets J-BAT would confront, each requiring different solutions and potentially different language in the authorizing Security Council resolution:

First, botnets with no State nexus; in other words, those that are purely criminal. These present the simplest case for taskforce action. States would be more willing to permit taskforce access to their local Internet networks to sinkhole a criminal syndicate preying on its citizens' bank accounts. States without the capability to locate and prosecute a botnet controller would likely be more willing also to allow taskforce personnel into their territory to perform these functions. It is worth noting that a Security Council resolution alone can be sufficient to create an obligation on a U.N. Member State to apply the measures identified by the Security Council.[241] States could be obligated, then, to cooperate with the taskforce.

Second, botnets with a suspected State nexus (e.g., GameOver Zeus). If a State publicly opposed taskforce action against a particular botnet, the State would appear to have an interest in utilizing the botnet. The progressive development of customary international law toward recognizing botnets as universally criminal and an illegitimate use of State power will drive a wedge between botnets and State actors which might otherwise employ a botnet for tactical convenience. Strong multilateral leadership from the U.N. Security Council is important for setting the defeat of botnets as a common goal.

[241] *See* U.N. Charter art. 41 ("The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures.").

Third, botnets controlled by a State actor (potentially Trickbot). These present the hardest challenge to the taskforce. First, they represent a possible source of opposition to the formation of a taskforce in the first place. Second, botnets formed and controlled by a State—especially if they continue to be used after the formation of the taskforce—would represent an alternate State practice, which could undermine the formation of a rule of customary international law disapproving of botnets. Nothing would prevent a State such as the United States from using its own resources to dismantle the botnet—especially if the U.N. Security Council had legitimized action against botnets in a Security Council resolution. However, the scenario of State-operated botnets would raise more difficult questions under international law. First, State use of a botnet would contravene the Budapest Convention if the State were a party or observer because operating a botnet necessarily "requires illegal access to computer systems."[242] Additionally, if the Security Council authorized J-BAT on the premise that botnets are a threat to international security, use of a botnet by a State would be impermissible under international law and a violation of a Member State's obligation to assist the Security Council in implementing the measures it has chosen to "maintain or restore international peace and security."[243] If a State continued to operate a botnet even after U.N.-sanctioned action against botnets, a multistate U.N.-sanctioned taskforce could be placed in the difficult position of deciding whether or not to enforce international law against a Member State. This could potentially set up questions of first impression for bodies like the International Court of Justice, including: is the action of dismantling a State's botnet—which may be viewed as an organ of that State—permissible under international law, and if so, is this cyber action a use of force under the U.N. Charter?[244]

As it did in confronting piracy by creating the CMF,[245] the United States could spur U.N. authorization of anti-botnet operations by leading the formation of J-BAT with partners and allies under the direction of CYBERCOM. Under this three-part frame-

[242] PROVISIONS OF THE BUDAPEST CONVENTION COVERING BOTNETS, *supra* note 172, at 4.

[243] See discussion of U.N. Charter art. 39 in Section III.B *supra*; a Member State's obligation to assist the Security Council in undertaking its determined measures arises under art. 43.

[244] *See* U.N. Charter art. 2(4) ("All Members shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any state . . . .").

[245] See discussion of CTF 151 in Section III.B *supra.*

work, CYBERCOM would ideally focus such an international effort on those purely criminal botnets in Category 1, allowing States falling in Categories 2 or 3 to conform over time to a rule of customary international law under which botnets are treated as internationally unlawful. From the U.S. perspective, focusing on criminal botnets would leave open the possibility of future cooperation with Russia and other States that are suspected of using botnets but may acquiesce to a no-botnet rule once it crystallizes. While some States may push back against accusations that one of their nationals is profiting from such a criminal enterprise,[246] placing botnet disruption within a multinational team under a rotating command would lend legitimacy to those allegations. Moreover, bringing the mission under U.N. auspices will allow the recalcitrant State's government to save face if it feels obligated to denounce a U.S.-led intervention against its citizens but could accept U.N. interventions.

Professor Stigall has argued for slackening the limits on a State's extraterritorial exercise of enforcement jurisdiction when that State falls victim to crime spilling across borders from a State that is "unable to effectively carry out basic functions" like "the arrest or prosecution of a criminal."[247] Stigall has also addressed a significant counterargument to relaxing constraints on enforcement jurisdiction, namely, that States' increased activity in others' territories "would increase the likelihood of international conflict."[248] But, as evidenced by heightened concern about what constitutes a cyber use of force, "transnational criminals are already in the process of creating those conflicts."[249] An exception to jurisdictional limits might be narrowed to conform with the "unable or unwilling" standard offered by Egan in a parallel context: J-BAT could only act against those botnets controlled by actors in States which are unwilling or unable to sinkhole them.[250]

Joint action against botnets is thus only an initial step in the progressive development of customary international law regarding State conduct in cyberspace, and it would inevitably create new questions in international law. But it is an initial step that brings the international community closer to an answer on what kinds of cyber actions should be permitted under international law. The

[246] Dembosky Interview, *supra* note 220.

[247] Stigall, *supra* note 55, at 6–7.

[248] *Id.* at 44.

[249] *Id.*

[250] *See* Egan, *supra* note 160; Stigall, *supra* note 55, at 45.

fear of additional unanswered questions should not deter action. As with efforts to repress piracy, which altered rules like a state's right of visit,[251] international actions for the common good frequently raise new questions and require adaptations to existing law.[252]

One advantage of focusing the international community's attention on the problem of botnets is that they are a concrete problem in cybersecurity, a nebulous field to many policymakers and members of the public alike. The more technical aspects of their operations notwithstanding, the notion that botnets can grow using any number of devices in the average modern home[253] is a relatively simple concept when one understands that anything connected to the Internet can be coopted by a botnet. Additionally, botnets have tangible impacts in many States around the world, wherever consumers have had their personal information compromised, or a company has suffered a ransomware attack, at the hands of a botnet.

The scale of the botnet problem also matches the large-scale payoff of its solution. After the GameOver Zeus botnet was defeated, for example, the type of bank account fraud it perpetrated vanished from the United States.[254] This defied researchers' belief that such a dramatic amount of "account-takeover fraud" was conducted by "dozens of gangs" of hackers.[255] In reality, a single botnet had been responsible for $100 million in losses.[256] Thus, taking down even one botnet can greatly reduce cybercrime in a State. For a State with an economy much smaller than that of the United States, the results would be felt even more widely.

B. *Toward Customary International Law on Botnets*

In establishing the contours of acceptable State behavior in cyberspace, States should set sustainable long-term rules, not merely combat short-term aggravators. Such rules of customary international law shape behavior and generate predictable expectations, thus fostering stability in the international system. For this

[251] See discussion in Section V *supra.* A warship is not ordinarily permitted under international law to board a foreign ship except in limited circumstances, including reasonable suspicion that the foreign ship is engaged in piracy. UNCLOS, art. 110(1)(a).

[252] See discussion of the uses of Security Council authority, including the formation of international criminal tribunals, *supra* note 90.

[253] See discussion of the Internet of Things, *supra* note 21.

[254] *See* Graff, *supra* note 193.

[255] *Id.*

[256] *Id.*

reason, a State practice of recognizing that botnets are a universal threat to peace and security (and, by implication, an illegitimate use of State power) is a necessary complement to authorized multilateral action against them in the form of J-BAT.

In the interest of stability, such cyber rules should be crafted to maintain the State's monopoly on the use of force[257] and to advantage status-quo powers. The practice of States should not be to encourage more non-State actors to exercise rights reserved to sovereign States. The fallacy in predicting success for 21st-century cyber privateers based on the success of 18th- and 19th-century privateers is that, historically, privateers advantaged *ascendant* powers with smaller navies.[258] If hackback were accepted as a legitimate tool by States like Germany or the United States—which have the capacity to stand up cyber units like the Bundeskriminalamt, CYBERCOM, the FBI, and the U.S. Cybersecurity and Infrastructure Security Agency—States with greater cyber capabilities would be acquiescing to asymmetric cyber conflict in the proliferation of harmful cyber tools wielded by non-State actors. While cyber privateers like Microsoft's Digital Crimes Unit may have the means to protect themselves (and others) in the hazardous landscape of cyberspace, ceding police powers to a non-State entity by court orders authorizing private action has the potential to set a dangerous precedent of State practice that will ultimately prove counterproductive to repressing cyber threats.

When piracy off the coast of Somalia first emerged as a threat to global shipping, a similar debate unfolded over whether to allow merchants to fend for themselves or agree upon government-led measures. In 1997, one commenter noted that resorting to private retaliation—"arming civilian vessels on the high seas"—would only lead to "escalation of weaponry[,] . . . greater casualties[,] and death."[259] Likewise, permitting more private hacking in cyberspace will inevitably lead to defenders exploiting more vulnerabilities and creating more malware to hit back at botnets and other cybercriminal adversaries. In the early 2000s, the international community chose to turn to a government-led taskforce to solve the piracy

[257] For an argument that states have been slow to reinforce their monopoly on the use of force, but are slowly "civilizing cyberspace" by controlling network connections and Internet policy within their "already demarcated" physical territories, see Demchak & Dombrowski, *supra* note 39, at 38–44.

[258] *See* Kessinger, *supra* note 113, at 8 ("The United States realized that if privateering was banned, its nascent navy would be no match for the greater naval might of countries such as Britain and France.").

[259] Fokas, *supra* note 61, at 447.

problem. It should do the same now to solve the botnet problem. This is not a criticism of well-meaning private efforts to clean up the Internet, but rather, a reckoning with the reality of allowing hackback to continue unchecked.

Moreover, customary international law is concerned with the actions of *States*, not *private actors*. Relinquishing police powers traditionally reserved to States prevents customary international law from forming at all. If corporations choose to treat botnets as a scourge of global commerce but States remain inactive on the problem, there is no creation of State practice, no *opinio juris*, and therefore, no customary international law on the matter.[260]

Universal jurisdiction was a legal innovation which allowed England, a dominant naval power, to extend enforcement of its municipal law—and propagate its normative view of what international law should be. Similarly, Great Britain's expanded application of the law of piracy—and its militarization of anti-piracy efforts—began in the mid-1800s, when the United Kingdom could claim naval superiority from the Atlantic to the Mediterranean to the South China Sea after defeating Napoleon, and sought to quell unpredictable threats to commerce.[261] Indeed, Rubin argues that inconsistencies in British practice in the 1800s lead one to conclude that much of maritime "law" developed in this period was rooted in policy choices rather than theories of "natural law."[262] Today, while there may not be similar hegemony among the States with strong cyber capabilities, there should at least be a desire among them to enforce policies that yield a stable order in cyberspace. Legal innovations are again needed to help the law evolve the means to address transnational problems that threaten global commerce and individual nations' security.

The argument in favor of the progressive development of customary international law regarding botnets is not meant to suggest that creating such law is simple, or to paper over the disagreements that exist between States. But the Sino-Russian "cyber sovereignty" model is not necessarily opposed to cooperation in defeating botnets. Those States in favor of greater cooperation (likely to be

[260] See discussion of customary international law in Section III.A *supra.*

[261] *See* RUBIN, *supra* note 59, at 201 ("British sea power emerging from the Napoleonic Wars so dominated international sea commerce that it is difficult throughout the nineteenth century to distinguish British interpretations of international law . . . from statements of international law persuasive on all states participating in the international legal order as defined in Europe."); *see generally id.* at 201–16 (describing the evolving applications of such law).

[262] *See id.* at 209.

those currently represented in J-CAT[263]) need not take a position on "cyber sovereignty" in order to make cooperation against botnets successful. They would merely ask for help from States like China and Russia to disconnect the command-and-control servers and "zombie" computers within their local networks. Rather than setting up a clash over competing models of "sovereignty," such cooperation can respect the positions of States like China and Russia while putting off for another day the more difficult discussion of resolving States' differences on the question of "cyber sovereignty."

Finally, the fact that Russia may have employed a botnet in its conflict with Ukraine[264] does not mean that Russia would not welcome the evolution of a rule that maintains the State's monopoly on police powers vis-à-vis private actors' ability to act in similar fashion. Global cooperation to defeat botnets could simultaneously reinforce the "cyber sovereignty" position while fostering a State practice of delegitimizing the use of botnets. As with counterpiracy efforts, cyberspace is a nuanced plane that ultimately requires cooperation to address common threats. There must be *some* tolerance for *some* number of contradictory outcomes. The reality of contradiction should not forestall honest efforts to create cyber rules that will ultimately benefit States and their citizens.[265] New technologies cannot always fit neatly into existing legal regimes, and "[s]ociety will likely be required to accept remedies that may, at times, be laced with conflicting values but are largely beneficial to humanity."[266] Botnets affect every State; they are a target around which the international community can rally and begin to cooperate in cyberspace. By synchronizing international efforts against a common enemy, the fight against botnets can also produce secondary benefits that help establish longed-for "rules of the road" in cyberspace.

[263] J-CAT is made up of EU and EU partner states. *See* discussion of J-CAT in Section VI.C *supra*.

[264] *See* Graff, *supra* note 193.

[265] Zoom interview with Brandon W. Jackson, Professorial Lecturer in Law at The George Washington University Law School (Nov. 13, 2020) (memorandum on file with *The George Washington International Law Review*) [hereinafter Jackson Interview].

[266] Brandon W. Jackson, *Artificial Intelligence and the Fog of Innovation: A Deep Dive on Governance and the Liability of Autonomous Systems*, 35 Santa Clara High Tech. L.J. 35, 62 (2019).

C. *Secondary Benefits: Promoting Attribution and Deconfliction*

Information sharing is critical to solving problems in cyberspace.[267] This is why the successful efforts against botnets to date have involved multiple entities and stakeholders across State borders.[268] Greater amounts of information make attribution possible because patterns in tactics, techniques, and procedures (TTPs) help identify different cyber actors.[269] With members of different States working side-by-side in a taskforce, information-sharing would be almost by osmosis: the attribution of States' actions in cyberspace would become readily apparent to the taskforce over time, and by communicating that information back to participating States, those States' own knowledge of other States' TTPs would be greatly improved. Notably, the China-led Code of Conduct also acknowledges the benefits of information-sharing and calls on signing States to "develop confidence-building measures [including voluntary exchange of information] aimed at increasing predictability and reducing . . . the risk of conflict."[270]

A greater ability to attribute cyber actions to a particular State means there would no longer be the delay or deniability that currently accompanies allegations that a particular State committed a particular cyber act.[271] When the United States claims that Russia committed a particular act (or vice-versa) the State could make that claim with a higher degree of confidence, having become familiar with the other State's TTPs by working side-by-side on anti-botnet operations.

A heightened ability to make accurate attribution has two main benefits: deconfliction and de-escalation. First, when operating in cyberspace, actors who recognize other actors' movements can adjust their own accordingly. This is not unlike the deconfliction practices of China and Russia vis-à-vis CTF 151 maneuvers in the Gulf of Aden.[272] Better familiarity with another actor's TTPs results in fewer collisions. Second, the ability to make faster attribution with a higher level of confidence promotes de-escalation by raising the cost of committing malicious cyber conduct. Deniability currently allows States and the cybercriminals behind

[267] Jackson Interview, *supra* note 265.

[268] *See* discussion of J-CAT in Section VI.C *supra.*

[269] *See* SOLARIUM COMM'N, *supra* note 5, at 112.

[270] Proposed Code of Conduct, *supra* note 200, at 6.

[271] *See* SOLARIUM COMM'N, *supra* note 5, at 27.

[272] *See* discussion of CTF 151 in Section III.B *supra.*

botnets to act in cyberspace with impunity.[273] They cannot be held accountable if no one can be sure that it is in fact they who are controlling an army of "zombie" computers. Attribution solves this accountability problem.

VIII. Conclusion

Greater cooperation in cyberspace could very well lead to fewer conflicts because it would raise the stakes of accountability. When a taskforce of multiple States, under a rotating command, can clearly identify a cybercriminal or State conducting malicious cyber behavior, criminals and States alike will think twice before sowing digital destruction.

Because it is a new and evolving domain, cyberspace requires establishing both a legal framework and customs which, though unwritten, are still a powerful predictor of behavior. But customary international law does not develop overnight. Where States are still in disagreement about where to begin in setting cyber "norms," the best place to start is a place where all—or at least, most—can agree. Botnets are a common threat to every Internet user in every State. For the most part, they are criminal enterprises not aligned with any State. Like pirates on the high seas, they are a scourge to global commerce that equally affect each computer—the digital equivalent of a ship. The same methods used to reduce pirate attacks in the Gulf of Aden can be applied now to rid the Internet of botnets. Failure to address botnets, which are the engine driving the growth of malware-as-a-service, will only allow a variety of Internet threats to fester and multiply. Botnets serve no benign purpose; like the pirates of old, "[i]n the immediate nearness of the gold, all else [is] forgotten" and they hope only "to seize upon the treasure . . . and sail away as [they] had at first intended, laden with crimes and riches."[274] Woe to those sailors who have no hope of rescue from the State.

[273] *See* Ahmad, *supra* note 45, at 6.

[274] Robert Louis Stevenson, Treasure Island 188 (Robert Frederick Ltd. ed. 1998).