Note

Transnational Cyber Offenses: Overcoming Jurisdictional Challenges

Alexandra Perloff-Giles†

INTRODUCTION

In his 1996 *Declaration of the Independence of Cyber Space*, cyber activist (and former Grateful Dead lyricist) John Perry Barlow vividly described the Internet as a place beyond national borders:

> Governments of the Industrial World, you weary giants of flesh and steel, . . . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. . . . Cyberspace

† Law clerk to the Hon. Marsha S. Berzon, Ninth Circuit Court of Appeals; Yale Law School, J.D. 2017; Harvard College, A.B. 2011. I am very grateful to Professors Joan Feigenbaum, Oona Hathaway, and especially Scott Shapiro, for providing the impetus for this Note and helpful suggestions throughout the writing process. I would also like to thank Peter Tzeng and my classmates in the Law and Technology of Cyber Conflict course, as well as Erin Biel, Valerie Comenencia Ortiz, Shikha Garg, Beatrice Walton, Mattie Wheeler, and the other editors of the *Yale Journal of International Law*, for their valuable feedback and careful editing.

> does not lie within your borders.[1]

As Barlow's declaration makes clear, cyberspace lacks geographic boundaries and does not map neatly onto the traditional system of territorial jurisdiction. While this jurisdictional dilemma has long been recognized,[2] few have examined its precise contours. Partly because of this failure to map the precise nature of the jurisdictional problem, regulation of the Internet is commonly seen as either empirically unfeasible or normatively illegitimate. Meanwhile, cyber threats have proliferated, accentuating the need to regulate cyber activity and to impose sanctions for cyber offenses.

This Note examines one category of cyber threat for which the problems of territorial jurisdiction are particularly acute: transnational cyber offenses. Transnational cyber offenses ripple across borders, exploiting the global, interconnected architecture of Internet communications. They affect multiple countries, their reach often difficult to cabin or predict. They may be carried out by individuals or non-State groups, affiliated or not with a government; they may target individuals, corporations, foreign media, State entities, or all of the above. By distinguishing transnational cyber offenses such as malware from other cyber threats such as cyberwarfare or ordinary computer crime, this Note invites regulators to develop and implement more creative, tailored solutions to address this increasingly common and disruptive form of attack.

Part I provides the technical background to illuminate why transnational cyber offenses represent a distinctive legal challenge. I describe the architectural design choices that shaped the modern cyber landscape; define transnational cyber offenses; and explain the technical features of common transnational cyber offenses. Part II shows *why* transnational cyber offenses in particular cannot be adequately regulated under the standard legal frameworks of domestic crime or war. Reassessing the much-debated issue of whether existing law applies to the cyber context, I contend that the proper question is not *whether* those frameworks apply but *when* they apply or *what kinds* of cyber hostilities existing frameworks can properly regulate. I show that, while both domestic criminal law and the international law of armed conflict may be appropriate legal frameworks for *some* cyber activity, neither properly applies to transnational cyber offenses.[3]

Finally, Part III offers possible legal solutions for holding perpetrators of transnational cyber offenses accountable. Without accountability measures, cyberspace risks becoming a Hobbesian state of nature in which victims engage in self-help and cyber-vigilantism. Recognizing the need for creative alternatives to either domestic criminal law or international humanitarian law, I look to both historical and contemporary models of international dispute

---

1. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), http://www.eff.org/cyberspace-independence.

2. *See generally* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

3. Long before the invention of the Internet, Philip Jessup coined the term "transnational law" to refer to law that "regulates actions or events that transcend national frontiers." PHILIP JESSUP, TRANSNATIONAL LAW 2 (1956). Cyber activities are quintessential transnational events.

resolution to offer novel solutions based on international civil arbitration, transnational criminal law, and international criminal law. As the number of transnational cyber offenses continues to escalate, and the nascent Internet of Things—a rapidly growing network of "smart" or Internet-connected devices—promises to raise the stakes of these threats, the stability and security of cyberspace depend upon the elaboration of an effective global accountability regime.

I. INTERNET ARCHITECTURE AND THE MECHANICS OF CYBER ATTACKS

A. Historical Overview of Internet Design

The same features of the Internet that were crafted to ensure its survivability in the Cold War era create security vulnerabilities today. Rather than taking an uninterrupted journey from one point to another, digital information makes many short trips as it navigates computer networks. This node network system opens up many more points of attack and allows attacks to spread widely across geographic boundaries. Put briefly, "[t]he origin of the threat posed by cyberspace is found in the architecture of the Internet itself."[4]

In the early 1960s, as the United States and the Soviet Union were building up their nuclear ballistic missile systems and became ensnared in the Cuban Missile Crisis, a nuclear attack seemed imminent. The central node of telephony systems, through which all communications passed, came to be regarded as "a single, very attractive target."[5] Consequently, U.S. officials and researchers sought alternatives to command and control communications systems that could withstand nuclear devastation.

Taking up that challenge, engineer Paul Baran developed a new communications network built upon the principles of redundancy and decentralization. In contrast to telephony systems, Baran's system relies on a distributed network, whereby each node is connected to multiple other nodes in a web. Information is routed from one node to another until it reaches its final destination in a process Baran referred to as "hot-potato routing."[6] Without a centralized switching facility, links can survive attacks on some of the switching nodes: if there is a problem or congestion at one node, information can simply route around it. In Baran's words, "[t]here is no central control; only a simple local routing policy is performed at each node, yet the over-all system adapts."[7] Compared to hierarchical systems, Baran's distributed

4. William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 252 (2011).

5. JANET ABBATE, INVENTING THE INTERNET 16 (1999) (quoting PAUL BARAN, 5 ON DISTRIBUTED COMMUNICATIONS: HISTORY, ALTERNATIVE APPROACHES, AND COMPARISONS 8 (1964)).

6. PAUL BARAN & SHARLA P. BOEHM, 2 ON DISTRIBUTED COMMUNICATIONS: DIGITAL SIMULATION OF HOT-POTATO ROUTING IN A BROADBAND DISTRIBUTED COMMUNICATIONS NETWORK (1964), http://www.rand.org/pubs/research_memoranda/RM3103.html.

7. Paul Baran, *On Distributed Communications Networks*, 12 IEEE TRANSACTIONS ON COMMUNICATIONS SYSTEMS 1, 8 (1964). The distributed network, made up of many short links connected by nodes, was made possible by the emergence of digital technology. Analog signals

network has the advantage, as he described it, of "survivability in the cases of enemy attack directed against nodes, links or combinations of nodes and links."[8]

Additionally, Baran's system divides information into packets, or what he termed "message blocks."[9] On older, circuit-switched networks like the analog telephone network, an act of communication takes up the entire circuit between two endpoints for the duration of the communication. Packet-switched networks like the modern Internet, by contrast, break communications into packets of data that get routed along potentially different paths before ultimately being reassembled at their final destination. In the Cold War context, the division of a single message into packets had the advantage of making it more difficult for spies to eavesdrop.[10]

Baran's research laid the groundwork for modern computer networking. After an initial phase in which the U.S. Department of Defense, and later the U.S. National Science Foundation, funded and managed the development of the Internet, public commercial use of the Internet began in 1989, and by 1995, the U.S. government relinquished control. The World Wide Web, an information-sharing medium built on top of the Internet's system of interconnected computer networks, helped bring the technology of the Internet to life. Embracing an ethos of openness, Timothy Berners-Lee and the other founders of the Web aspired to a model of "radically democratic" social organization in place of governmental or corporate control.[11]

Since then, Internet technology has grown organically and transformed nearly every aspect of contemporary life. Today, the topology of the Internet routing system consists of over 59,000 individual networks,[12] situated within dozens of large networks that control routing and that extend across geographic borders.[13] Whereas the Internet was once accessible only through desktop computers whose locations were fixed and traceable, wireless devices now abound. Fiber optic cables crisscross the Atlantic Ocean, transmitting ever more data at ever higher speeds. And the advent of cloud computing, whereby data is stored on a privately-owned or a public third-party cloud, rather than on local computers, further accentuates the tension between national sovereignty and the borderless nature of online activity.

The Internet as we know it thus reflects a deliberate repudiation of centralized, top-down authority. Its technological infrastructure was built to

---

degenerated when they moved between links and became increasingly distorted, whereas digital signals could be regenerated at each node, preventing distortion. *See* ABBATE, *supra* note 5, at 16.

8. Baran, *supra* note 7, at 1.

9. *Id.* at 6.

10. ABBATE, *supra* note 5, at 19.

11. *See* Jemima Kiss, *An Online Magna Carta: Berners-Lee Calls for Bill of Rights for Web*, GUARDIAN (Mar. 12, 2014), http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

12. *See* CIDR REPORT, http://www.cidr-report.org/as2.0/ (last visited Nov. 12, 2017) (providing an up-to-date count of autonomous systems or ASes—collections of Internet Protocol routing prefixes operating under a single administrative authority—in the inter-domain routing system).

13. *Id.*

prioritize survivability and flexibility over security; as it has evolved, that infrastructure has become ever more global and more reliant upon shared resources. How, then, can cyberspace be regulated in the twenty-first century? How do we balance the freedom and openness of the Internet with rules—and authorities empowered to enforce those rules? In short, how can we maintain order in a virtual space that, by design, is not subject to the control of any single jurisdiction?

B. Transnational Cyber Attacks Defined

As the previous Section showed, the designers of the Internet considered the possibility of harm to the physical infrastructure of the Internet and built systems that would continue to operate if one node were destroyed. They failed, however, to consider the possibility of damage caused by the very data being communicated.[14] Transnational cyber offenses work from within: they use the language of code to infiltrate systems, disrupt service, and compromise data.

Transnational cyber offenses share three defining features. First, they are deliberate offenses: they require some willful act from which it is reasonably foreseeable that harm will result. (There may be circumstances in which negligent failure to take reasonable cyber security measures could give rise to liability,[15] but a computer technician who inadvertently disrupts his company's network temporarily has not committed a transnational cyber offense.)

Second, transnational cyber offenses are quintessentially *cyber* offenses: they take advantage of the design characteristics of the Internet described above. Offenses by a single perpetrator against a single victim that merely employ digital tools—for example, an identity thief hacking into a person's computer to steal credit card information, a corporation engaging in industrial cyber espionage against a competitor, or one country penetrating another country's nuclear controllers to disable weapons development—are not transnational cyber offenses. Rather, those offenses can all exist in the kinetic world—a thief stealing the credit card of an unsuspecting victim, a corporate spy sneaking in to obtain trade secrets, a country bombing or otherwise disabling another country's nuclear weapons facility. Similarly, crimes such as money laundering and child pornography may use the Internet, but they can also exist without the Internet; nothing about them depends upon a networked architecture. Transnational cyber offenses, by contrast, are particular to cyberspace: indirect and easily transmitted, they exploit the decentralized, networked nature of the web to cause harms that have no kinetic-world equivalent.

Third, transnational cyber offenses are *transnational.* Like other

14. *See, e.g.*, Stahl, *supra* note 4, at 254 ("The routing system's structure was intended to ensure the Internet's continuing functionality in the event of an external attack, but it was not designed to prevent damage caused by the very data that it transfers.").

15. *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553 (2005).

transnational offenses such as environmental crime or illicit traffic in drugs and arms, transnational cyber offenses involve more than one country in their "inception, perpetration and/or direct or indirect effects."[16] They are, in other words, what Kofi Annan called "problems without a passport."[17] They may be carried out by a government or by non-State actors and may affect individuals, government entities, corporations, non-governmental organizations, or other groups. Crucially, however, they present challenges that transcend borders and that, for a variety of reasons, cannot be addressed by any one nation alone. Attacks may be launched from any location with Internet access; attackers can hide their location with anonymizing services;[18] and the Internet reduces the transaction costs of cross-border cooperation in planning and executing attacks.[19] Further, Internet traffic, designed to travel through the *fastest* route, may not always take the most geographically *direct* route: a single piece of malicious code may be routed through multiple countries.[20] Moreover, because of the packet system, whereby different packets can take different routes, the potential for information to traverse different jurisdictions is multiplied.[21] Network architecture makes it difficult for Internet users to predict the territorial jurisdictions of which they are potentially availing themselves[22]: "the ease, speed, and unpredictability with which data flows across borders make its location an unstable and often arbitrary determinant of the rules that apply."[23] Finally, transnational cyber offenses often have a wide reach, such that the impact of an attack can be felt far from either the initial launch point or the target first hit.[24] In short, the configuration of cyberspace allows offensive acts

16. Ninth U.N. Congress on the Prevention of Crime & the Treatment of Offenders, *Interim Report by the Secretariat*, ¶ 9, U.N. Doc. A/CONF.169/15/Add.1 (Apr. 4 1995).

17. Press Release, Secretary General, Environmental Threats Are Quintessential "Problems Without Passports," Secretary General Tells European Environment Ministers, U.N. Press Release SG/SM/6609 (June 23, 1998).

18. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 331 (2015).

19. Kamala D. Harris, California Attorney General, *Gangs Beyond Borders: California and the Fight Against Transnational Organized Crime*, OFF. CAL. ATT'Y GEN. 59 (March 2014), http://oag.ca.gov/sites/all/files/agweb/pdfs/toc/report_2014.pdf ("[W]hile in the past criminal cross-border cooperation was cumbersome, expensive, and vulnerable to law enforcement, the Internet and other advances in high-speed international communication have dramatically reduced these 'transaction costs.' Now, far-flung criminal network operatives can exploit new criminal opportunities from their desktops without even having to leave their homes—let alone their home countries.").

20. *See* Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 9 DUKE L. & TECH. REV. ¶ 60 (2010).

21. *Id.* ¶ 25.

22. Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 56 ("The physical location of electronic evidence . . . often depends upon the fortuity of network architecture: an American subsidiary of a French corporation may house all of its data on a server that is physically located in France; two Japanese citizens might subscribe to America Online and have their electronic mail stored on AOL's Virginia servers.").

23. Daskal, *supra* note 18, at 329; *see also id.* at 367 ("[D]ata can move from Point *A* to Point *B* in circuitous and arbitrary ways, all at breakneck speed.").

24. Kristin M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CONG. RES. SERV., R41927, at 5 (Jan. 17, 2013) ("Due to the global nature of the Internet and other rapid communication systems, crimes committed via or with the aid of the Internet can quickly impact victims in multiple state and national jurisdictions."); PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS 92 (2012) ("[I]n an electronically connected world the effects of any given action may immediately be felt elsewhere with no relationship to physical geography at all.").

to originate, move through cyber space, and affect their targets in ways that are distinctly transnational.

C. Common Types of Transnational Cyber Attacks

Infectious malware and denial-of-service are two common examples of transnational cyber offenses. The first, malware, is code designed to inflict harm on data, hosts, or networks. Malware typically infects a computer system when a user accesses a corrupt website or downloads an email attachment. The two most familiar forms of malware—viruses and worms—spread easily from one computer to another. Viruses insert themselves into an executable file or program, lying dormant until a user runs the infected program; they then get passed on when the program is transferred to another computer via e-mail, CD-ROM, USB key, or some other file-sharing system. Worms, by contrast, are standalone software; they can replicate independently within a host computer and can travel unaided to other computer systems connected by a network or the Internet. Both forms of malware thus capitalize on features of the cyber landscape, whether interoperability or Internet connectivity, to disseminate threats to potentially unknown victims.

An increasingly common variant of malware is ransomware—computer malware that spreads covertly and holds victims' computer data hostage by locking their screens ("locker ransomware") or by encrypting their files ("crypto ransomware"). Once inside the system, crypto ransomware creates encrypted copies of files that can be opened only with a decryption key, deletes the original files, and leaves instructions demanding a ransom payment to access the key. According to one estimate, as many as forty percent of companies worldwide have been targeted by ransomware attacks.[25]

A second common transnational cyber offense is a denial-of-service (DoS) attack. In a DoS attack, a perpetrator launches a barrage of fake requests from a single source, overwhelming the target computer system, server, or network. Unlike malware, which changes the functionality of the target system, DoS attacks temporarily block access to the target system. Malware and denial-of-service can be combined to create a distributed denial-of-service (DDoS) attack. Perpetrators of DDoS attacks use malware to hijack and enslave numerous computers called "zombies" that flood target networks with traffic. Fake requests issued by the network of zombie computers or devices—known as a "botnet"—can disable target systems for several hours, or even days.[26] The

25. Victoria Woollaston, *WannaCry Ransomware: What It Is and How To Protect Yourself*, WIRED (May 22, 2017), http://www.wired.co.uk/article/wannacry-ransomware-virus-patch. Governments are also increasingly susceptible to such attacks: state and local government networks are reportedly nearly twice as likely to be infected with malware or ransomware as small or medium-sized businesses. *Malware, Ransomware Twice As Likely To Hit State, Local Networks*, GCN (Dec. 1, 2015), http://gcn.com/articles/2015/12/01/sled-ransomware.aspx.

26. DDoS attacks can take place either at the application layer (Layer 7), or at the network or transport layer (Layer 3 or 4). Application layer attacks flood a server with requests such as HTTP floods or DNS query floods that drain all computing resources and prevent the server from answering legitimate requests. Network or transport layer attacks send malicious requests over different network protocols, consuming all available bandwidth and shutting down most network infrastructures. *See* Nat'l

use of zombie armies or "tiered" botnets enables hackers to execute attacks "across many different, geographically dispersed computer servers" rather than from "a single point of command."[27] In many cases, the attacker can remotely control zombie devices without the device owner even knowing his or her device was hijacked: Vint Cerf, one of the fathers of the Internet, once estimated that up to one-fourth of all networked computers may be part of botnets.[28]

Recent history is rife with examples of transnational cyber offenses that caused significant global impact yet were carried out with impunity. Perhaps the most notorious is the so-called "Love Bug" attack. As a student at the Amable Mendoza Aguiluz (AMA) Computer University in the Philippines, Onel de Guzman wrote a program designed to steal Internet passwords. In May 2000, the "ILOVEYOU" virus—so-named for the phrase displayed in the subject line of each contaminated e-mail—began attacking millions of Microsoft Windows computers, scanning computers for log-in names and passwords, destroying image and sound files, and spreading via e-mail attachment to everyone in the targeted user's address book. The virus, which caused an estimated ten billion dollars in damage,[29] reportedly penetrated the computer systems of at least fourteen federal agencies in the United States, foreign governments such as the British Parliament, the Belgian banking system, U.S. state governments, international organizations like the International Monetary Fund, media outlets like the *Washington Post* and ABC News, credit unions, and large corporations like AT&T and Ford Motor Company.[30]

Internet Service Providers traced the virus to de Guzman.[31] Philippine law enforcement initially pressed charges, but the Philippine Department of Justice was ultimately forced to drop the case because Philippine law at the time did not prohibit computer hacking.[32] Meanwhile, the U.S. Department of Justice charged de Guzman in absentia but could not extradite him, as extradition treaties require dual criminality and de Guzman's actions were not illegal under

---

Cybersecurity & Commc'ns Integration Center, *DDoS Quick Guide*, U.S. DEP'T OF HOMELAND SEC. (Jan. 29, 2014), http://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf.

27. SUSAN W. BRENNER, CYBERTHREATS 2 (2009).

28. *See* Tim Weber, *Criminals "May Overwhelm the Web,"* BBC NEWS (Jan. 25, 2007), http://news.bbc.co.uk/2/hi/business/6298641.stm.

29. Kevin Poulsen, *May 4, 2000: Tainted "Love" Infects Computers*, WIRED (May 3, 2010), http://www.wired.com/2010/05/0504i-love-you-virus.

30. *The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack: Hearing Before the Subcomm. on Tech. of the H. Comm. on Sci.*, 106th Cong. 12 (2000) (statement of Keith A. Rhodes, Director, Office of Computer and Information Technology Assessment).

31. Shannon C. Sprinkel, Note, *Global Internet Regulation: The Residual Effects of the "ILOVEYOU" Computer Virus and the Draft Convention on Cyber-Crime*, 25 SUFFOLK TRANSNAT'L L. REV. 491, 492 (2002).

32. The Philippines quickly tried to correct its mistake. On June 14, 2000, Philippine President Joseph Estrada signed the Electronic Commerce Act, outlawing computer crimes. However, because the Act did not apply retroactively, it could not cover de Guzman. *See* Mark Landler, *A Filipino Linked to 'Love Bug' Talks About His License To Hack*, N.Y. TIMES (Oct. 21, 2000), http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html.

the law of the Philippines.[33] Thus, de Guzman escaped punishment.

Since then, there have been countless other denial-of-service and malware attacks with similarly devastating consequences. The 2007 attacks on Estonian websites disrupted emergency services for over an hour and implicated zombie computers in as many as 178 countries.[34] The October 2016 Dyn attack on U.S.-based data centers disrupted access to news sites and major commercial websites and caused ripple effects not only across the United States, but also in Europe.[35] Most recently, in May 2017, the WannaCry ransomware attack infected an estimated 230,000 computers in more than 150 countries.[36] Impacting Russia especially severely, the WannaCry ransomware infected telecommunications and utility companies, banks, universities, government offices, electronic payment machines at gas stations and rail companies, and more.[37] In England, the ransomware severely disrupted the National Health Service, preventing doctors from accessing patient files and forcing hospitals to turn people away at the emergency room.[38]

At the dawn of the Internet of Things, DDoS attacks are poised to become an even bigger threat. More and more everyday objects and devices, from thermostats and coffee pots to clothing, heart monitors, cars, and even roads, are becoming or could soon be embedded with sensors and connected to the Internet.[39] As the number of Internet-connected devices grows, not only are there more potential targets for attackers but the potential size and force of zombie botnets also increases.[40]

---

33. Under the double or dual criminality principle of extradition law, a person may be extradited "only if the acts charged are criminal by the laws of both countries." *Collins v. Loisel*, 259 U.S. 309, 311 (1922); *see also* SATYA D. BEDI, EXTRADITION IN INTERNATIONAL LAW AND PRACTICE 69-84 (1966) (characterizing the dual criminality principle as a rule of customary international law). The United States' extradition treaty with the Philippines, like virtually all extradition treaties, contains a dual criminality clause. Extradition Treaty Between the Government of the United States of America and the Government of the Republic of the Philippines, Phil.-U.S., art. 2(1), Nov. 13, 1994, S. TREATY DOC. NO. 104-16 (1995).

34. *See* MARCEL H. VAN HERPEN, PUTIN'S WARS: THE RISE OF RUSSIA'S NEW IMPERIALISM 140 n.25 (2d ed. 2015); Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

35. Three waves of DDoS attacks flooded Dyn, a key Domain Name System provider, with DNS look-up requests, blocking access to major online commerce, social media, and news websites. *See* Tess Owen, *What You Need To Know About Friday's Massive Cyber Attack*, VICE NEWS (Oct. 23, 2016), http://news.vice.com/story/what-you-need-to-know-about-fridays-massive-cyber-attack.

36. Peter Dockrill, *Experts Warn the Global "WannaCry" Ransomware Hack Is Far From Over*, SCIENCEALERT (May 1, 2017), http://www.sciencealert.com/experts-are-warning-the-global-wannacry-ransomware-hack-isn-t-over; David E. Sanger, Sewell Chan & Mark Scott, *Ransomware's Aftershocks Feared as U.S. Warns of Complexity*, N.Y. TIMES (May 14, 2017), http://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html.

37. *See, e.g.*, *Ransomware Cyber-Attack: Who Has Been Hardest Hit?*, BBC (May 15, 2017), http://www.bbc.com/news/world-39919249; Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NPR (May 15, 2017), http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

38. *See, e.g.*, *Global Cyberattack Strikes Dozens of Countries, Cripples U.K. Hospitals*, CBS NEWS (May 12, 2017), http://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack.

39. *See* MICHAEL MILLER, THE INTERNET OF THINGS: HOW SMART TVS, SMART CARS, SMART HOMES, AND SMART CITIES ARE CHANGING THE WORLD (2015).

40. *IoT Devices Being Increasingly Used for DDoS Attacks*, SYMANTEC (Sept. 22, 2016),

In short, the architectural interconnectivity of the Internet and the ability of threats to propagate in cyberspace create "collective vulnerability."[41] With malware worms rapidly infecting computers an ocean away, denial-of-service attacks blocking access to websites for users anywhere in the world, and DDoS attacks hijacking swarms of slave computers, questions of who has the authority to respond and how perpetrators can be held accountable are urgent. By recognizing transnational cyber offenses as a distinct category, we can begin to formulate legal solutions that fit the technological realities, rather than trying to fit quintessentially digital problems into standard regulatory frameworks.

II. BEYOND DOMESTIC CRIMINAL LAW AND INTERNATIONAL HUMANITARIAN LAW: TRANSNATIONAL CYBER OFFENSES AND THE PROBLEM OF JURISDICTION

In the physical world, "we divide threats into internal ('crime') and external ('war') and assign responsibility for each to a separate institution (law enforcement and the military)."[42] In the cyber context, we have largely replicated that division: in the United States, computer crime is prosecuted by the Federal Bureau of Investigation (FBI), while cyberwarfare is under the purview of the Defense Department. But that division between internal and external threats maps awkwardly onto the cyber context where, as Susan Brenner notes, "what we define as 'internal' threats can now come from external, civilian actors."[43]

The bulk of the scholarly literature on cyber threats has hewed to this traditional division. Computer crime is written about by criminal law scholars and criminologists, while cyberwarfare is seen as the purview of international lawyers and national security experts. Some scholars, recognizing that the law of war is a blunt instrument, have concluded that we need a new "comprehensive . . . solution to the emerging threat of cyber-attacks."[44] This Note advocates for a more nuanced approach. I argue that, rather than attempting to apply any one existing legal framework to all cyber threats, we ought to be more attentive to the particular characteristics of each cyber threat. Just as there is no single body of law for all wrongful acts in the physical world, so, too, there is no single body of law for all wrongful acts in cyberspace. The question is not simply *what* body of law applies but *when*.

For ordinary cybercrimes with kinetic world analogues, such as child pornography or financial fraud, domestic criminal law is generally appropriate. When the perpetrator of such crimes is located in the same jurisdiction as the victim, prosecution is relatively straightforward. For other, rare kinds of cyber

---

http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

41. ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 95-96 (2010).

42. Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 207, 210 (Jack M. Balkin et al. eds., 2007).

43. *Id.*

44. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 822 (2012).

hostilities—namely, highly destructive attacks by one government against another government—the law of armed conflict offers an appropriate legal framework.

Transnational cyber offenses, however, do not fit comfortably within either category. Cyber criminals' ability to collaborate internationally, to launch cyber operations remotely, and to execute attacks with global effects complicates the application of domestic law. At the same time, borderless, transnational attacks on computers and on the civilian information infrastructure do not look like traditional warfare between States. Transnational cyber offenses are typically undertaken by private individuals or non-State groups, not States,[45] and to the extent they are attributable to national governments, few such incidents meet the threshold for an armed conflict.[46] Transnational cyber offenses thus fall into a legal lacuna, neither adequately covered by domestic criminal law, nor subject to international humanitarian law. In this Part, I discuss the limitations of these two traditional legal frameworks when it comes to the regulation of transnational cyber offenses.

A. The International Humanitarian Law Framework and Its Limitations

International law offers potentially useful guidance for addressing cyber offenses carried out by one State against another State. Some human rights treaties may speak to elements of cybercrimes. For example, the right to privacy recognized in international human rights documents like the Universal Declaration of Human Rights[47] or the International Covenant on Civil and Political Rights[48] could be understood to prevent unlawful access to other people's private data, while the right to freedom of expression and freedom of information in those documents arguably prohibits interfering with access to media websites.[49]

More often, international law approaches to cyber offenses have focused on *jus ad bellum* and *jus in bello*. *Jus ad bellum* determines when a State may lawfully use force against another State. Under Article 51 of the U.N. Charter, an "armed attack" allows States to engage in self-defense—that is, to respond with a "use of force," notwithstanding Article 2(4)'s general prohibition on the "use of force against the territorial integrity or political independence of any [S]tate."[50] Regardless of the legality of the use of force, international

45. Mary Ellen O'Connell, *Cyber Security Without Cyber War*, 17 J. CONFLICT & SECURITY L. 187, 206 (2012).

46. *See infra* note 51 and accompanying text.

47. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/810, art. 12 (Dec. 10, 1948) [hereinafter UDHR].

48. International Covenant on Civil and Political Rights art. 17, *adopted* Dec. 19, 1966, S. EXEC. DOC. E, 95-2 (1978), 999 U.N.T.S. 171 [hereinafter ICCPR].

49. *See* UDHR, *supra* note 47, art. 19; ICCPR, *supra* note 48, art. 19.

50. U.N. Charter art. 2, ¶ 4; *id.* art. 51; *see also* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 286 (C. Czosseck et al. eds., 2012) ("[A]n 'armed attack' is an action that gives States the right to a response rising to the level of a 'use of force,' as that term is understood in the jus ad bellum.").

humanitarian law (or *jus in bello*) applies whenever an armed conflict arises. According to the now-classic formulation of the International Criminal Tribunal for the former Yugoslavia in the celebrated *Tadić* case, an international "armed conflict exists whenever there is a resort to armed force between States."[51] Codified notably in the post-World War II Geneva Conventions and their Additional Protocols, the law of armed conflict was designed to regulate traditional horizontal warfare between States. In the archetypal case, international armed conflict arises "when parts of the armed forces of two [or more] States clash with each other."[52] In such a case, "[a]s soon as the armed forces of one State find themselves with wounded or surrendering members of the armed forces or civilians of another State on their hands, as soon as they detain prisoners or have actual control over a part of the territory of the enemy State, then they must comply with the [Geneva Conventions]."[53]

In the context of cyber conflict, however, the question arises whether cyber operations can constitute an "armed attack" under Article 51, permitting a State to respond in self-defense, or a "resort to armed force," triggering the existence of an international armed conflict.[54] As to the former, Marco Roscini points out that "both the scale *and* the effects of the use of force . . . determine the occurrence of an armed attack."[55] Thus, an intentional power grid outage, a deadly crash engineered by hacking into aircraft computers, or a shutdown of computers controlling waterworks and dams, thereby causing flooding in populated areas, could all rise to the level of an armed attack, while a DDoS attack temporarily disrupting non-critical infrastructure would not.[56] As to the existence of an international armed conflict, Michael Schmitt, director of the Tallinn Manual Project, maintains when a cyber attack is carried out by a State and is "either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable," international "humanitarian law principles apply . . . even though classic armed force is not being employed."[57] The International Committee of the Red Cross (ICRC) goes

51. Prosecutor v. Tadić, Case No. IT-94-1-A, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

52. Dietrich Schindler, *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols*, 163 RCADI 117, 131 (1979).

53. Hans-Peter Gasser, *International Humanitarian Law: An Introduction*, *in* HUMANITY FOR ALL: THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT 491, 510-11 (Hans Haug ed., 1993).

54. There is disagreement as to whether a "resort to armed force"—i.e., the threshold for determining the existence of an international armed conflict under the law of armed conflict—is tantamount to a "use of force" under Article 2(4) of the U.N. Charter, *see* MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 128-32 (2014), and as to whether a "use of force" under Article 2(4) is tantamount to an "armed attack" under Article 51, *see Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13, 21-22 (2012).

55. ROSCINI, *supra* note 54, at 73.

56. *See id.*; Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 105 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

57. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 IRRC 365, 374 (June 2002) (emphasis omitted).

further, taking the position that physical damage or destruction is not required; cyber operations need only disable an object to qualify as a use of armed force subject to international humanitarian law rules.[58] Still, there must be *some* intensity threshold for disabling or disruption, such that the effects are analogous to those of destruction by traditional armed force.[59] Thus, even cyber operations targeting government facilities or critical infrastructure such as hospitals or power grids may or may not qualify as a "resort to armed force," depending on their impact. In short, very few, if any, cyber events to date would meet the threshold for an international armed conflict or qualify as "armed attacks" permitting States to respond with either cyber or kinetic force in self-defense.

The second major challenge in applying international humanitarian law principles to cyber hostilities is the application of the State responsibility doctrine. Historically, if an attack was carried out by a foreign power, there was little doubt regarding State responsibility; soldiers were uniformed, and only nations had the resources to carry out attacks in another country. Cyber attacks, however, can be carried out at low cost by States, by hacker groups with ties to foreign governments, or simply by individuals whose identities and geographic locations are frequently hidden.[60] Holding a nation responsible for an attack is significantly more difficult in the cyber world than in the physical world.

Notwithstanding these challenges, for a narrow set of cyber operations, international humanitarian law offers the most appropriate legal framework. The Stuxnet attack on the Natanz nuclear enrichment facilities—perhaps the most prominent cyber attack to date—is one such example. Stuxnet was a targeted direct attack on a nuclear facility operated by the Iranian government.[61] It is widely thought to have been carried out by the United States and Israel. (Although neither State has officially assumed responsibility, experts point out that no non-State actor has, and few States have, the capacity to build and deploy Stuxnet.[62]) Moreover, Natanz operated on a closed computer system. Because the target was not connected to the public Internet, the attack did not cause the kinds of ripple effects that characterize transnational cyber offenses.[63] Indeed, buried inside the code was a "do-not-

58. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Report 31IC/11/5.1.2, INT'L COMMITTEE OF THE RED CROSS 37 (Oct. 2011), http://e-brief.icrc.org/wp-content/uploads/2016/08/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf.

59. ROSCINI, *supra* note 54, at 135.

60. *See* Michael Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SECURITY L. 245, 246 (2012).

61. *See, e.g.*, John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 3-4, 21 (2011).

62. Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 22 (2015).

63. Overseen by Iranian engineers, the Natanz computer network involved a supervisory control and data acquisition—or SCADA—control system whereby process commands are issued and activity monitored by a supervisory computer system. In a SCADA system, centralized computers monitor and regulate industrial-control systems that in turn monitor machinery operations such as uranium enrichment "by adjusting, switching, manufacturing, and controlling key processes based on digitized feedback of data gathered by sensors." David Maimon & Alexander Testa, *On the Relevance*

infect" indicator; when the virus encountered a computer that did not fit the target profile, the virus destroyed itself, minimizing incidental or "knock-on" effects.[64] The Stuxnet attack therefore fits within familiar paradigms of States carrying out carefully targeted, politically motivated strikes against other States—and, according to some scholars at least, Stuxnet rose to the level of an Article 51 armed attack.[65] So, while determinations of intensity and attribution can be challenging, *jus ad bellum* and *jus in bello* provide the right framework for analyzing—and potentially responding to—incidents like Stuxnet. For most transnational cyber offenses, however, the perpetrators and the victims are not (or not exclusively) States, the offense does not constitute an Article 51 "armed attack" or a "resort to armed force," and the international humanitarian law framework is unavailing.

B. The Domestic Criminal Law Framework and Its Limitations

In addition to the law of armed conflict, the other legal framework often applied to cyber operations is domestic criminal law. Domestic criminal law is a tool for the "protection of public mores within a specific locality"[66]: it functions effectively when a crime takes place in a particular jurisdiction, which is able to regulate the activity, investigate the crime, and punish the perpetrator. Conventional crimes that are committed by a resident of the country where the crime takes place and that happen to make use of computers—for example, identity theft, fraud, copyright violations, child pornography, cyber stalking, and online bullying—may be effectively regulated by domestic criminal law.

Domestic criminal law is ill-adapted, however, to transnational cyber offenses, which have effects beyond the reach of a State's police power.[67] Law enforcement agencies are candid about the difficulties of policing crimes that implicate multiple jurisdictions. Testifying before Congress, then-FBI Assistant Director Thomas Kubic evoked the challenges of the Westphalian nation-state model of jurisdiction as applied to transnational cyber threats:

> In the past, a nation's border acted as a barrier to the development of many criminal enterprises, organizations and conspiracies. . . . [T]he advent of the Internet . . . has erased these borders. . . . Subjects located in other countries are

---

of Cyber Criminological Research in the Design of Policies and Sophisticated Security Solutions Against Cyberterrorism Events, *in* THE HANDBOOK OF THE CRIMINOLOGY OF TERRORISM 553, 555 (Gary LaFree & Joshua D. Freilich eds., 2016).

64. Gregg Keizer, *Stuxnet Code Hints at Possible Israeli Origin, Researchers Say*, COMPUTERWORLD (Sept. 30, 2010), http://www.computerworld.com/s/article/9188982/Stuxnet_code_hints_at_possible_Israeli_origin_researchers_say.

65. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 342, 384 (Michael N. Schmitt ed., 2013) (noting disagreement among the Tallinn Manual drafters on whether Stuxnet represented an armed attack).

66. Cameron S.D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 INT'L J. CYBER CRIMINOLOGY 55, 62 (2015).

67. *See* Bertrand de La Chapelle & Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, INTERNET & JURISDICTION 7 (Apr. 2016), http://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf ("[O]verlapping and often conflicting territorial criteria make both the application of laws in cyberspace and the resolution of Internet-related disputes difficult and inefficient.").

> increasingly targeting victims in the U.S. utilizing the Internet. Evidence can be stored remotely in locations not in physical proximity to either their owner or the location of criminal activity. In addition, losses suffered by victims in individual jurisdictions may not meet prosecutive thresholds even though total losses through the same scheme may be substantial. In order to subpoena records, utilize electronic surveillance, execute search warrants, seize evidence and examine it in foreign countries, the FBI must rely upon local authorities for assistance. In some cases, local police forces do not understand or cannot cope with technology. In other cases, these nations simply do not have adequate laws regarding cyber crime and are therefore limited in their ability to provide assistance.[68]

As Kubic observes, cross-border activity was historically rare: territoriality established "the bedrock principles for the development of modern international law."[69] But in the Internet era, cross-border activity is ubiquitous, and the transnational nature of many cyber offenses is at odds with those bedrock territoriality principles. Territorial jurisdiction is generally understood to have three dimensions: legislative or prescriptive jurisdiction (the jurisdiction to prescribe legal rules); judicial or adjudicative jurisdiction (the jurisdiction to resolve disputes); and executive or enforcement jurisdiction (the jurisdiction to enforce judgments).[70] Transnational cyber offenses are problematic along all three dimensions.

When it comes to legislative jurisdiction, different countries have different laws governing cybercrime. If the territoriality principle of international law permits any State to exercise regulatory control over transnational events "sufficiently closely linked or connected" to that State,[71] any State that experiences the effects of online activity could exercise jurisdiction. In this way, a single act could potentially subject the perpetrator to the substantive laws of several, perhaps even dozens of, jurisdictions. But, as James Brierly remarked long before the emergence of the Internet, "the suggestion that every individual is or may be subject to the laws of every State at all times and in all places is intolerable."[72] Internet users have not meaningfully consented to be governed by other countries' norms, particularly given the unpredictability of Internet data routing. As Jennifer Daskal explains, "[i]t is widely understood that when one travels to . . . a foreign jurisdiction,

---

68. *Fighting Cyber Crime: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 107th Cong. 51-53 (2001) (prepared statement of Thomas T. Kubic, Principal Deputy Assistant Director, Criminal Investigative Division, FBI).

69. *See* KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 11 (2009).

70. *See, e.g.*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (AM. LAW INST. 1987) (describing categories of jurisdiction).

71. Uta Kohl, *Jurisdiction in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 30, 33 (Nichlas Tsagourias & Russell Buchan eds., 2015) (emphasis omitted).

72. James L. Brierly, *The "Lotus" Case*, 44 L.Q. REV. 154, 162 (1928); *see also, e.g.*, AARON SCHWABACH, INTERNET AND THE LAW: TECHNOLOGY, SOCIETY, AND COMPROMISES 161 (2d ed. 2014) ("Internet content is thus potentially subject to the law of every jurisdiction on the planet."); *id.* at 163 ("[T]he advent of the Internet makes multiple-jurisdiction transactions the norm rather than the exception. . . . If disputes arise from the transaction, any or all of the states and countries involved might conceivably have jurisdiction over the matter."); Adria Allen, *Internet Jurisdiction Today*, 22 NW. J. INT'L L. & BUS. 69, 75 (2001) ("Cyberlaw jurisdictional theorists are faced with the reality that a simple homespun web page could be subject to jurisdiction by all of the nearly three-hundred sovereigns around the world.").

one is subject to that sovereign nation's laws," but if an individual sends data over the Internet, which happens to transit through another nation, "that individual is not consciously choosing to bind himself to any particular foreign government's laws."[73]

Subjecting every online actor to the law of every State, under a theory that activity on the Internet can be experienced anywhere, cannot be the solution to the problem of transnational cyber offenses. But what country's law should apply? Should any country in which malware is downloaded have jurisdiction? Only countries hosting servers that the malware passes through? Only the country where the perpetrator was physically located when the attack was launched? Choice of law rules do not offer ready answers—some rules provide for jurisdiction over acts that affect that territory, while others provide for jurisdiction over conduct set in motion in that territory—and countries are unlikely to forego jurisdiction over incidents affecting their own citizens.[74]

Even as legislative jurisdiction may be over-inclusive in the context of cyber activity, it may also be under-inclusive. Laws must apply extraterritorially for a State to bring charges for criminal acts initiated outside its territorial limits. When cybercrime legislation does not apply extraterritorially, attackers can forum shop for favorable jurisdictions where their activities are not proscribed. As Claude Lombois put it vividly, "the reach of the police officer is only as long as his arm . . . . [H]e is a constable only at home."[75]

Most domestic cybercrime laws, including in the United States, do not apply extraterritorially;[76] extraterritorial exercises of authority are typically seen to infringe upon the sovereignty of other countries.[77] In recent years, the United States has somewhat expanded its legislative and adjudicative jurisdiction, extending the reach of U.S. laws and empowering U.S. courts to hear some cases involving foreign parties. In 2001, Russians Vasiliy Gorshkov and Alexey Ivanov were found responsible for stealing data and extorting money from U.S. businesses.[78] In order to prosecute them, the U.S. government created a fake computer security firm, "Invita," and invited Gorshkov and Ivanov to come to Seattle to interview with the firm.[79] The FBI promptly arrested both of them.[80] Gorshkov was tried and sentenced in Washington,[81]

---

73. Daskal, *supra* note 18, at 367-68.

74. *See, e.g.*, Andre R. Jaglom, *Liability On-Line: Choice of Law and Jurisdiction on the Internet, or Who's In Charge Here?*, TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT LLP 10, http://www.thsh.com/documents/liabilityon-line.pdf.

75. CLAUDE LOMBOIS, DROIT PENAL INTERNATIONAL 536 (2d ed. 1979), *translated in* Pierre Trudel, *Jurisdiction Over the Internet: A Canadian Perspective*, 32 INT'L LAWYER 1027, 1047 (1998).

76. *See* Hathaway et al., *supra* note 44, at 874 ("The majority of the existing criminal laws bearing on cyber-attack do not apply extraterritorially—that is, they do not reach criminal activity occurring outside the United States.").

77. Anthony J. Colangelo, *What Is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303, 1311-12 (2014).

78. United States v. Ivanov, 175 F. Supp. 2d 367, 373 (D. Conn. 2001); United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

79. Robert Lemos, *FBI "Hack" Raises Global Security Concerns*, CNET (Mar. 28, 2002), http://www.cnet.com/news/fbi-hack-raises-global-security-concerns.

80. *Id.*

while Ivanov's case was transferred to Connecticut,[82] where the district court determined that the relevant statutes *did* apply extraterritorially and that, "because the intended and actual detrimental effects of Ivanov's actions in Russia occurred within the United States," Ivanov could be tried and sentenced in the United States for crimes committed outside the country.[83] Still, the successful prosecutions of Gorshkov and Ivanov under U.S. law are the exception, not the norm. Put simply, a territorial approach to jurisdiction over transnational cyber offenses leads, in theory, to *too many* countries exercising legislative and adjudicative jurisdiction—and, in practice, to *too few*.

The third dimension of territorial jurisdiction—enforcement jurisdiction—is also problematic for transnational cyber offenses, as other countries may be unable to provide the necessary digital evidence or unwilling to cooperate with investigations and extradition. First, enforcing cybercrime statutes requires expertise and resources that not all States have. Developing nations may lack the capacity to adequately investigate and prosecute cybercrimes or even to assist in cross-border investigations, even if they have the legal authority to do so and are willing to comply. Meanwhile, even technologically sophisticated nations may fail to provide effective assistance. Mutual Legal Assistance Treaties (MLATs)—agreements between two or more countries to provide assistance on criminal legal matters—are key tools for dealing with cross-border evidence requests. But MLATs are of limited efficacy in the cyber context[84]: they typically require dual criminality (that is, the act must be criminalized in both the requesting and receiving countries),[85] and are only useful when countries have explicitly entered bilateral arrangements—a requirement at odds with the global nature of the Internet. MLAT requests are also slow to process. The United States, for instance, takes an average of ten months—and sometimes much longer—to comply with valid electronic evidence records requests from other countries pursuant to MLATs.[86] Such waiting times represent "an eternity in Internet time"[87] and can not only delay investigations and prosecutions but also lead to the potential loss of fragile digital evidence.[88]

Second, countries may deliberately thwart enforcement of another country's criminal law. Without the cooperation of foreign governments in

---

81. *See Gorshkov*, 2001 WL 1024026, at *4.

82. One of the companies whose computers he had hacked was located in Vernon, Connecticut. *Ivanov*, 175 F. Supp. 2d at 368.

83. *Id.* at 370-75.

84. Susan Brenner has described MLATs as "so unsuitable as to be almost futile with regard to cybercrime and cybercriminals." Brenner, *supra* note 42, at 209.

85. *See* R.E. Bell, *The Prosecution of Computer Crime*, 9 J. FIN. CRIME 308, 317 (2002); *see also supra* note 33.

86. *Liberty and Security in a Changing World*, PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMM. TECH. 227 (Dec. 12, 2013), http://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

87. *See* Curtis E.A. Karnow, *Counterstrike*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 135, 138 (Jack M. Balkin et al. eds., 2007).

88. *See* Brenner, *supra* note 42, at 213 ("Digital evidence is fragile and can easily be destroyed or altered."); MOHAMED CHAWKI ET AL., CYBERCRIME, DIGITAL FORENSICS AND JURISDICTION 20 (2015) ("[N]etwork traffic is transient and must be captured while it is in transit.").

gathering and processing digital forensic evidence located abroad and in executing warrants and subpoenas, a country can struggle to give effect to its domestic laws. More problematic still is the extradition of foreign citizens. The refusal by countries like Russia and China to extradite their citizens has repeatedly proven an obstacle to prosecution,[89] as it did initially with Gorshkov and Ivanov, before the U.S. government concocted its clever scheme.[90] Often, the United States issues arrest warrants or indicts cybercriminals in absentia, without the perpetrators ever facing jail time. For example, in 2014, the United States indicted five Chinese military hackers on charges of economic espionage in its first ever indictment of State actors for cyber theft;[91] an FBI cybercrime investigator later admitted that "[t]he chance of us ever getting those Chinese guys is about zero."[92] Enforcement of monetary penalties is similarly difficult: the country that issues a judgment may be unable to enforce the judgment if the perpetrator is not physically located there and does not hold assets there. As Jack Goldsmith explains:

> [A] nation can only enforce its laws against: (i) persons with a presence or assets in the nation's territory; (ii) persons over whom the nation can obtain personal jurisdiction and enforce a default judgment against abroad; or (iii) persons whom the nation can successfully extradite. . . . The large majority of persons who transact in cyberspace have no presence or assets in the jurisdictions that wish to regulate their information flows in cyberspace. . . .[93]

In short, even if legislative and adjudicative jurisdiction can be established and a judgment is entered against the perpetrator, there is little real threat of

---

89. *See, e.g.*, Mansur Mirovalev & Colin Freeman, *Russian Hacker Wanted by US Hailed as Hero at Home*, TELEGRAPH (June 7, 2014), http://www.telegraph.co.uk/news/worldnews/europe/russia/10883333/Russian-hacker-wanted-by-US-hailed-as-hero-at-home.html (explaining that there is little likelihood of prosecuting a Russian national who reportedly distributed malware causing over $100 million in economic losses); *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*, U.S. DEP'T OF JUSTICE (Mar. 15, 2017), http://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions (noting that one of the FBI's Cyber Most Wanted criminals escaped to Russia to avoid extradition); Message from the President of the United States Transmitting the Agreement Between the Government of the United States of America and the Government of Hong Kong for the Surrender of Fugitive Offenders, S. TREATY DOC. NO. 105-3, at iii (1997) (noting "the absence of an extradition treaty with the People's Republic of China").

90. Ariana Eunjung Cha, *A Tempting Offer for Russian Pair*, WASH. POST (May 19, 2003), http://www.washingtonpost.com/archive/politics/2003/05/19/a-tempting-offer-for-russian-pair/2c6a5407-8378-4939-8491-038efab2c5fb ("Not having an extradition treaty with Russia made the hackers case more difficult to prosecute, says Stephen Schroeder, who worked on the case as a U.S. attorney.").

91. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEP'T OF JUSTICE (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (quoting Eric Holder stating that the case "represents the first ever charges against a state actor for this type of hacking").

92. Adam Goldman & Matt Apuzzo, *U.S. Faces Tall Hurdles in Detaining or Deterring Russian Hackers*, N.Y. TIMES (Dec. 15, 2016), http://www.nytimes.com/2016/12/15/us/politics/russian-hackers-election.html.

93. Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216-17 (1998). For Goldsmith, the limits of enforcement jurisdiction—i.e., the fact that in practice there is often no real threat of extraterritorial legal liability—obviates the problem of overly broad legislative jurisdiction. But, to the extent one believes in law as a constraining force, reliance upon the fact that foreign laws may reveal themselves ex post to apply but cannot be enforced is unsatisfying. *See* David G. Post, *Governing Cyberspace: Law*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 883, 893 (2008).

extraterritorial legal liability.

Domestic criminal law is thus often an ineffectual tool when it comes to bringing foreign cyber criminals to justice. Domestic criminal law works when a perpetrator commits a crime in one jurisdiction, which is empowered to investigate the crime and arrest the perpetrator. Transnational cyber offenses cross borders, giving rise to jurisdictional overlap and conflict. For such offenses, "[t]he actions of individual states are insufficient"[94]: solutions lie beyond domestic criminal law.

III. ACCOUNTABILITY FOR TRANSNATIONAL CYBER OFFENSES: INTERNATIONAL DISPUTE RESOLUTION

As the previous Parts have shown, neither international humanitarian law nor domestic criminal law effectively regulates or deters transnational cyber offenses. In the face of this challenge, some scholars have thrown up their hands, concluding that cyberspace is "a largely ungovernable space,"[95] while computer scientists have prioritized preventive security measures.[96] While prevention is, of course, essential, it must be coupled with some form of accountability if we wish to avoid a Hobbesian reality in which victims of cyber attacks take it upon themselves to hack back.[97] Put bluntly, if there is not a forum where businesses can bring complaints and receive some relief, victims of cyber attacks will increasingly resort to cyber-vigilantism.[98]

It is difficult to know how frequently victims engage in self-help given the uncertain legality of hacking back.[99] For well over a decade, companies have complained that passive defense measures are insufficient to combat cyber threats and have attempted self-defense measures.[100] According to a 1999

94. Abraham D. Sofaer & Seymour E. Goodman, *Cyber Crime and Security: The Transnational Dimension, in* THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 1, 30 (Abraham D. Sofaer & Seymour E. Goodman eds., 2001).

95. MARINELLA MARMO & NERIDA CHAZAL, TRANSNATIONAL CRIME AND CRIMINAL JUSTICE 66 (2016).

96. *See* Joan Feigenbaum et al., *Systematizing "Accountability" in Computer Science* 1 (Yale Dep't of Comput. Sci. Tech. Report No. 1452, 2012), http://dedis.cs.yale.edu/dissent/papers/tr1452.pdf ("Traditionally, computer-science researchers have taken a preventive approach to security and privacy in online activity." (emphasis omitted)); Joan Feigenbaum et al., *Accountability and Deterrence in Online Life (Extended Abstract), in* PROCEEDINGS OF THE 3RD INTERNATIONAL WEB SCIENCE CONFERENCE (2011), https://dl.acm.org/citation.cfm?id=2527031 ("The standard technical approach to privacy and security in online life is preventive." (emphasis omitted)).

97. *See* THOMAS HOBBES, THE LEVIATHAN (1651) (describing the state of nature as a war of all against all).

98. A decade ago, Curtis Karnow described a growing interest in hacking back, based on the premise that "only a computer can react fast enough to . . . disable the attacking machine." Karnow, *supra* note 87, at 140. Conversations at the Spring 2017 Yale Cyber Leadership Forum made clear that the interest in self-help has only increased. Yale Cyber Leadership Forum, Yale University (Mar. 30-Apr. 1, 2017) (notes on file with Author).

99. *See, e.g.*, COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RES. COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 207 (William A. Owens et al. eds., 2009).

100. *See, e.g.*, Paul A. Strassman, *New Weapons of Information Warfare*, COMPUTERWORLD (Dec. 1, 2003), http://www.strassmann.com/pubs/computerworld/new-weapons.shtml ("Current methods of blocking intruders aren't likely to be adequate to secure Internet commerce . . . . The cost of launching attacks will decrease and the expense for defenses will escalate until it becomes prohibitive

survey of Fortune 500 companies, approximately thirty percent of companies had installed software that could launch counterattacks, and many of the companies surveyed said they would rather rely on such counterstrikes than involve law enforcement,[101] which some companies feared could affect their reputation and stock price.[102] Moreover, "[h]ighly skilled private groups—untethered from the many constraints and rules that bind governments—often can be more nimble in pursuing bad actors in cyberspace."[103] Hack-back tools to fight fire with fire have now become commercially available;[104] there is even an underground market where banks and other large corporations can hire contractors to shut down their attackers.[105]

But, as Major General Brett Williams, former director of operations for Cyber Command, noted, "[t]he fact that it's very easy for a civilian to take actions that are normally reserved for law enforcement or military doesn't make it right."[106] Cyber-vigilantism is problematic for the same reason vigilantism in the kinetic world is problematic[107]: vigilantes can botch the attack and alert offenders; vigilantes are not privy to government strategy and may interfere with legitimate law enforcement; vigilantism lacks the procedural safeguards that ensure accuracy in identifying the offender;[108] punishments inflicted by vigilantes may not be proportionate to the initial offense; and, most importantly, vigilantes lack the accountability that lies at the heart of democratic society. Put simply, "[i]t would be dangerous and short-sighted to delegate the roles of police, judge, jury, and punisher to private parties that exist outside of the democratic system."[109]

---

for companies to pursue the current policy of adhering to static defensive measures."); Jay P. Kesan & Ruperto P. Majuca, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 3 (Ill. Pub. Law and Legal Theory Research Papers Series, Working Paper No. 08-20, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932 ("[M]any firms feel that simply protecting one's computer network with a defensive boundary is not adequate given today's hostile Internet environment . . . [and] feel that hacking back is necessary in order to prevent further degradation to the firm's systems and to deter or reform the hacker.").

101. Barbara Gengler, *Strikeback*, 1 COMPUTER FRAUD & SECURITY 8, 8-9 (1999).

102. Kesan & Majuca, *supra* note 100, at 2.

103. Jeff Kosseff, *The Hazards of Cyber-Vigilantism*, 32 COMPUTER L. & SECURITY REV. 642, 643 (2016).

104. In 2004, network infrastructure security company Symbiot Security Inc. launched a program that offered several levels of graduated response to attacks. *See* Raksha Shetty, Associated Press, *Networks Lash Back at Cyber Hacks*, CBS NEWS (June 18, 2004), http://www.cbsnews.com/news/networks-lash-back-at-cyber-hacks/. That same year, Lycos Europe briefly released a screensaver that, when used, launched DDoS attacks on spam websites. *See* Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 33 (2006).

105. Wyatt Hoffman & Ariel (Eli) Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 14, 2017), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236.

106. Major Gen. Brett Williams, *Why Cyber-Vigilantism Cannot Be Tolerated*, MSNBC (Jan. 13, 2015), http://www.msnbc.com/the-last-word/watch/why-cyber-vigilantism-cannot-be-tolerated-383995459547.

107. *Cf.* United States v. Fraser, 647 F.3d 1242, 1246 (10th Cir. 2011) ("Ours is not the rule of vigilante justice but the rule of law.").

108. *See, e.g.*, United States v. Morris, 549 F.3d 548, 551 (7th Cir. 2008) (noting that vigilantes "might botch their investigation, alerting the offender in time for him to elude justice").

109. Kosseff, *supra* note 103, at 643.

This Part sketches possible solutions to the problem of regulating transnational cyber offenses. Drawing upon existing models of international dispute resolution and imagining new roles for international institutions, I offer proposals for both civil and criminal liability. Crucially, these proposals are not mutually exclusive: a robust accountability regime could combine an international arbitration scheme to make victims whole with criminal prosecution to deter cyber criminals. The same attentiveness to the particularities of a given attack that counsels against reflexive reliance on either domestic criminal law or international humanitarian law also motivates the elaboration of a multi-pronged set of solutions. Transnational cyber offenses can vary in intensity and geographic reach, can be conducted by individuals or non-State actors, and can hit individuals, corporations, state entities, and international organizations, among other victims. The appropriate legal tool may be different from one case to the next; the aim of this Part is not to prescribe but to propose new tools for the toolbox.

A. International Arbitration and Civil Liability

International arbitration offers one little-considered mechanism for holding perpetrators of cyber attacks accountable. Even before the modern international arbitration regime emerged, countries used civil arbitration to regulate transnational activity and resolve disputes. International arbitration is not only for disputes between nations, however. International civil arbitration can also be used to hold private actors accountable, without impermissibly undermining State sovereignty.[110]

Today, international commercial arbitration operates under the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958, more commonly known as the New York Convention.[111] As of November 2017, 157 nations had ratified the Convention.[112] Aimed at promoting international uniformity in the recognition and enforcement of arbitral awards, the New York Convention imposes two sets of rules on the national courts of member States. First, under Article II(3), national courts in member States must recognize arbitration agreements made between the parties. When confronted with a dispute governed by an arbitration agreement,

110. For example, under treaties Britain entered into with other nations in the nineteenth century, slave trade vessels could be seized by British vessels, and a so-called "mixed court" with arbitrators from each country would decide whether the seizure was lawful. *See* Eugene Kontorovich, *The Constitutionality of International Courts: The Forgotten Precedent of Slave-Trade Tribunals*, 158 U. PA. L. REV. 39 (2009). If the seizure was unlawful, the "Seizor" was liable for payments. *See, e.g.*, An Act for Carrying Into Effect a Treaty Between Her Majesty and the Republic of Bolivia for the Abolition of the Slave Trade 1843, 6 & 7 Vict. c. 14, arts. XVII-XIX.

111. United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38 [hereinafter New York Convention]. One commentator has described the Convention as "the most effective instance of international legislation in the entire history of commercial law." Michael John Mustill, *Arbitration: History and Background*, 6 J. INT'L ARB. 43, 49 (1989).

112. *List of Contracting States*, N.Y. ARB. CONVENTION, http://www.newyorkconvention.org/list+of+contracting+states (last visited Nov. 21, 2017).

courts must refer the parties to arbitration if either party so requests.[113] Second, under Article III, the Convention requires States parties to recognize and enforce arbitral awards issued in the territory of another State.[114] The Convention thus enables prevailing parties to collect on the assets of the losing party, even when the latter resides in another jurisdiction.

The New York Convention's widely adopted system of civil accountability for transnational wrongs could be harnessed to promote accountability for transnational cyber offenses. In the commercial context, businesses often agree to arbitration under the New York Convention, not only because arbitral awards are enforceable worldwide, but also because arbitration offers an efficient and confidential process with judges experienced in the subject area and no possibility for appeal. In turn, making this dispute-resolution channel available to businesses is an important reason why so many States have chosen to ratify the Convention, despite having to sacrifice a degree of sovereignty in the enforcement of foreign arbitral awards. In the cyber context, software companies and Internet Service Providers could require, as part of their terms of service, that disputes relating to cyber attacks be subject to arbitration. And because virtually every country in the world—including countries like Russia that are seen as cybercrime havens—has been hit by malware and DDoS attacks, countries may be incentivized by their own citizens and corporations to recognize the jurisdiction of an international arbitral body.

Significantly, there is precedent for tying a specialized arbitral scheme to the New York Convention. The Court of Arbitration for Sport (CAS), founded in 1984, harnesses the machinery of the New York Convention to resolve international sports-related disputes and to punish violators of international norms quickly, impartially, and cost-effectively.[115] The CAS is widely regarded as the final decision-maker for international sports-related disputes, "to the exclusion of national courts."[116] Once the CAS renders a judgment, sports organizations can enforce the judgment directly—for example, through bans on registering or playing—or parties can apply to national courts, typically the Swiss Federal Supreme Court, for enforcement under the New York Convention.[117]

We might imagine a specialized arbitral tribunal for cyber-related

---

113. New York Convention, *supra* note 111, art. II(3).

114. *Id.* art. III.

115. *See* Matthieu Reeb, *The Role and Functions of the Court of Arbitration for Sport (CAS), in* THE COURT OF ARBITRATION FOR SPORT 1984-2004, at 31, 31-39 (Ian S. Blackshaw et al. eds., 1st ed. 2006). Athletes before the CAS may also be subject to criminal proceedings in national courts. Louise Reilly, *An Introduction to the Court of Arbitration for Sport (CAS) & the Role of National Courts in International Sports Disputes*, 2012 J. DISP. RESOL. 63, 63, 77.

116. Reilly, *supra* note 115, at 67; *see also* Tribunal fédéral [TF] [Federal Supreme Court] May 27, 2003, III Arrêts du Tribunal Fédéral Suisse [ATF] 129 445 (Switz.), *translated in* 3 DIGEST OF CAS AWARDS 2001-2003, at 674 (Matthieu Reeb ed., 2004). As with any arbitral proceeding, the parties must consent to have their dispute heard by the CAS. Generally, consent arises out of an arbitration clause inserted into a contract, into the statutes or regulations of sports-related associations, or into the entry forms that athletes often sign to participate in sports events. *See* Reilly, *supra* note 115, at 66-67.

117. Reilly, *supra* note 115, at 76 & n.66.

disputes, analogous to the CAS. A cyber arbitration body could issue civil penalties for cyber infractions, with enforcement tied to the New York Convention such that a cyber attacker's assets could be seized wherever they may be located. Just as CAS arbitrators generally have recognized expertise in sports and sports law, so too an arbitral tribunal for cyber issues could benefit from arbitrators with technology expertise.

A cyber arbitration scheme could also be tailored to the unique features of transnational cyber offenses. Individuals, corporations, or States could all sue perpetrators. Class actions could also be permitted, allowing parties affected by a malware or ransomware attack to aggregate their claims to meet harm thresholds and, conceivably, to financially wipe out cyber villains. We could even envision liability for parties that negligently fail to secure critical infrastructure or fail to comply with cyber hygiene requirements, thereby permitting their devices to become part of botnets.

There is already one international body within which a cyber arbitration forum could reside. Under the aegis of the United Nations, the International Telecommunication Union (ITU) is a specialized agency that promotes international cooperation relating to telecommunications infrastructure and global technical standards. With a membership of 193 countries and nearly eight hundred private entities, the ITU has used its technical expertise to support less technically sophisticated countries and to engage in Internet-related research and development.[118] For example, the ITU in 2014 announced the creation of a Global Cybersecurity Index to evaluate and compare cybersecurity strategies worldwide.[119] Additional ITU activities include building capacity and helping countries establish national Computer Incident Response Teams.[120] As a result of initiatives like these, there has been talk in recent years of the ITU taking on a bigger role in Internet regulation.[121]

Proposals for the ITU to regulate the Internet have prompted outcries from those concerned that such regulation would destroy the open, decentralized governance system envisioned by Paul Baran and other pioneers of the early Internet.[122] At worldwide telecommunications conferences in 2012 and 2014, a number of countries, including Russia and Saudi Arabia, rejected proposals to expand the ITU's role in Internet governance, supposedly "to

---

118. *About International Telecommunication Union*, INT'L TELECOMM. UNION, http://www.itu.int/en/about (last visited Nov. 19, 2017); *ITU's 150 Years of Innovation*, ITU NEWS, May-June 2015, at 27-29, http://www.itu.int/en/itunews/Documents/2015_ITUNews03-en.pdf.

119. *Global Cybersecurity Index (GCI) 2017*, INT'L TELECOMM. UNION iii, 3 (July 19, 2017), http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

120. *CIRT Programme*, INT'L TELECOMM. UNION, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx (last visited Nov. 29, 2017).

121. *See, e.g.*, Johannes Thimm & Christian Schaller, *Internet Governance and the ITU: Maintaining the Multistakeholder Approach—The German Perspective*, COUNCIL ON FOREIGN REL. (Oct. 22, 2014), http://www.cfr.org/report/internet-governance-and-itu-maintaining-multistakeholder-approach; Jyoti Panday, *An Over-The-Top Approach to Internet Regulation in Developing Countries*, ELECTRONIC FRONTIER FOUND. (Oct. 23, 2017), http://www.eff.org/deeplinks/2017/10/over-top-approach-internet-regulation-developing-countries.

122. Rebecca Mackinnon, *The United Nations and the Internet: It's Complicated*, FOREIGN POL'Y (Aug. 8, 2012), http://foreignpolicy.com/2012/08/08/the-united-nations-and-the-internet-its-complicated.

correct historical imbalances resulting from the perceived dominance of the [United States] over the internet."[123] If international resistance could be overcome, however, the ITU would seem to be a natural entity to call upon to develop cyber regulations and to arbitrate disputes. A 2016 meeting of the ITU Telecommunication Standardization Sector saw some significant compromises on Internet governance, including agreements that governments should take on a "broader policy role";[124] that global, interoperable processes for sharing information about cybersecurity incidents should be promoted;[125] and that the ITU should assist member States in establishing a framework for "rapid response to major incidents."[126]

Two non-profit entities responsible for ensuring the reliable operation of the Internet could also take on a bigger role in cyber security and cyber dispute resolution. The Internet Engineering Task Force, an international open standards organization, develops voluntary standards for the Internet to promote interoperability and usability. The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the global Domain Name System (DNS), performs technical maintenance on DNS root zone registries, and manages IP address space. ICANN currently administers the Uniform Domain-Name Dispute-Resolution Policy (UDRP), a system for resolving disputes related to trademarks and Internet domain name registration. The UDRP administrative adjudication process could serve as a model for arbitrating disputes involving transnational cyber offenses. As of October 1, 2016, ICANN is no longer subject to U.S. government oversight,[127] potentially making it more likely that other countries would accept a greater regulatory role for ICANN.

Whether tied to an existing entity like the ITU or ICANN or entirely independent, an international civil arbitration system that allows victims of transnational cyber offenses to seek redress for losses could obviate the temptation to hack back. Further, the potential for individual victims to aggregate claims and obtain significant damages awards could meaningfully deter would-be cyber attackers. Of course, erecting an international arbitration system for cyber actions would present its own set of challenges that would have to be overcome—including developing an arbitration agreement analogous to the CAS and requiring or incentivizing Internet users to agree to submit to arbitration. Still, international civil arbitration tied to the New York

123. Sheetal Kumar, *Cybersecurity: What's the ITU Got To Do With It?* (July 9, 2015), http://www.gp-digital.org/cybersecurity-whats-the-itu-got-to-do-with-it (internal quotation marks omitted).

124. *ITU WTSA 2016 Outcomes: An Internet Society Perspective*, INTERNET SOC'Y 1 (Nov. 22, 2016), http://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-WTSA16-Outcomes-20161122.pdf (internal quotation marks omitted).

125. World Telecomm. Standardization Assembly, *Resolution 50 – Cybersecurity*, TELECOMM. STANDARDIZATION SECTOR OF ITU 4 (2016), http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-E.pdf.

126. *Id.* at 5.

127. Press Release, ICANN, Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends (Oct. 1, 2016), http://www.icann.org/news/announcement-2016-10-01-en.

Convention offers one possible new weapon in the legal arsenal for combating transnational cyber offenses.

B. Transnational Criminal Law

In addition to civil remedies for victims, a robust liability scheme for transnational cyber offenses ought also to include criminal penalties. As Section II.B demonstrates, relying on individual States to apply their penal law is inadequate. Countries without strong legal sanctions for cyber criminals can—either advertently or inadvertently, by design or by neglect—become havens for cybercrime.[128] One solution is therefore to harmonize laws across countries and to promote international cooperation on law enforcement, developing a transnational criminal law regime. While purely domestic crimes are criminalized only at the election of the State, and international law crimes create individual penal responsibility under international law, transnational criminal law indirectly creates criminal liability by imposing obligations on States to enact certain domestic penal laws.[129]

Legal harmonization is an important part of developing a transnational criminal law for transnational cyber offenses. At a minimum, every country ought to enact laws prohibiting core cybercrimes, such as the deliberate release of malware. But international cooperation at the level of enforcement is also important. Countries should commit to assist one another with real-time collection of traffic data, and technologically sophisticated countries should provide training to less technologically advanced countries. Additionally, provided there is reasonable cause for suspicion, countries in which evidence is found should be required to turn over evidence, such as computer hard drives, for investigation in other countries that may wish to attempt to decrypt files. A global agency, similar to Interpol, could also be charged with developing digital forensics techniques and conducting investigations to support national prosecutions. These proposals for developing international law norms of information-sharing and for assimilating those norms into domestic law suggest how transnational criminal law could promote accountability: countries would have to sacrifice a degree of State sovereignty as a precondition for more effective prosecutions of transnational cyber offenses.

Proposals for increasing criminal enforcement of cyber offenses are often met with concerns about attribution.[130] In fact, the problem of attribution may be overstated. To be sure, the architecture of the Internet is built to ensure anonymity, complicating *technical* attribution. But *legal* attribution, even in the kinetic world, often relies upon the accumulation of multiple incomplete pieces

---

128. Brenner, *supra* note 42, at 209.

129. *See generally* NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW (2012) (providing an overview of the features of developing transnational criminal law); Neil Boister, *Transnational Criminal Law?*, 14 EUR. J. INT'L L. 953 (2003) (coining the term "transnational criminal law").

130. *See, e.g.*, P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 73 (2014) ("Perhaps the most difficult [cybersecurity] problem is that of attribution.").

of evidence, forensic tools with less-than-perfect accuracy, inferences, analysis of motive, and judgment.[131] Those same strategies can be applied in the cyber context to find individuals criminally liable "beyond a reasonable doubt."[132] To the extent a prosecution in one country depends upon evidence obtained in another country that reveals sensitive information about the latter country's information-gathering capacities, States could commit to requiring that courts review sensitive evidence *in camera* and to sealing the court records.[133] While evidentiary issues in the cyber context are no doubt complex, attribution is a nuanced process that could benefit from the skills and resources—both technical and non-technical—of States acting together.

Some efforts to foster international cooperation along these lines are already underway. In 1997, the G-8 countries established the "24/7 Network of Contact Points" ("24/7 Network") for data preservation. Presently consisting of approximately seventy member countries, the G-8 24/7 Network allows countries to solicit the urgent assistance of other countries in cybercrime matters in order to preserve data for subsequent transfer through mutual legal assistance agreements.[134] The 24/7 Network is just a first step; the United Nations General Assembly has repeatedly called for a global framework to protect cyber infrastructure and combat cybercrime.[135] Several countries have also formed interjurisdictional task forces to address transnational cybercrime,[136] and the ITU has drafted model cybercrime legislation and compiled resources to assist countries in drafting their own cybercrime laws and procedural rules.[137]

The most important step toward a transnational criminal law for cyber offenses to date is the Budapest Convention on Cybercrime.[138] Drafted by the

---

131. *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 6 (2014) (explaining that attribution is an art as well as a science).

132. The standard of proof for a civil liability scheme such as that discussed in Section III.A, *supra*, would presumably be lower; as I suggest, strict liability may even be appropriate for failure to secure critical infrastructure or to comply with cyber hygiene rules. *See supra* p. 213.

133. Examples of judicial procedures for ensuring the confidentiality of information include the Foreign Intelligence Surveillance Act (FISA) courts in the United States, closed material procedures (CMPs) pursuant to the Justice and Secrecy Act in the United Kingdom, and special magistrate procedures pursuant to the Act on Shielded Witnesses in the Netherlands.

134. Leslie R. Caldwell, Assistant Attorney General, Remarks at the CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders, U.S. DEP'T OF JUSTICE (June 6, 2016), http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-ccips-csis-cybercrime-symposium-2016. The Office of International Affairs within the Department of Justice's Criminal Division saw a 1,000 percent increase in formal requests for computer records stored in the United States between 2000 and 2016. *Id.*

135. *See, e.g.*, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, G.A. Res. 58/199 (Jan. 30, 2004); Creation of a Global Culture of Cybersecurity, G.A. Res. 57/239 (Jan. 31, 2003); Combating the Criminal Misuse of Information Technologies, G.A. Res. 56/12 (Jan. 23, 2002); Combating the Criminal Misuse of Information Technologies, G.A. Res. 55/63 (Jan. 22, 2001).

136. Deb Shinder, *What Makes Cybercrime Laws So Difficult To Enforce*, TECHREPUBLIC (Jan. 26, 2011, 4:05 AM PST), http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce.

137. *See* Int'l Telecomm. Union, *ITU Toolkit for Cybercrime Legislation* (2010), http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf.

138. Council of Europe Convention on Cybercrime, *opened for signature* Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2006), E.T.S. No. 185 (entered into force July 1, 2004) [hereinafter

Council of Europe and adopted in 2001, the Budapest Convention has so far been ratified or acceded to by fifty-six States, largely European nations but also the United States, Canada, Australia, Israel, and Japan.[139] It represents, in former Secretary of State John Kerry's words, "[t]he best . . . legal framework for working across borders to define what cyber crime is and how breaches of the law should be prevented and prosecuted."[140]

The Budapest Convention assumes that criminal prosecutions will continue to take place at the level of the State but aims to harmonize national laws and promote international cooperation on evidence-gathering. Member States have jurisdiction over any offense that occurs in their territory, regardless of where the attacker is located. Additionally, States have jurisdiction over offenses committed by their nationals, provided that the offense was punishable under the criminal law of the State where it was committed or was committed outside the territorial jurisdiction of any State.[141] Further, the Convention facilitates mutual assistance and extradition by allowing for the Convention itself to be used as an extradition or legal assistance treaty in the absence of any preexisting MLAT between the relevant States.[142]

While the Budapest Convention is an important step, so far it remains largely symbolic. Many important States, including Brazil, Russia, India, and China, have refused to join the Budapest Convention. Russia—the only Council of Europe nation not to have signed—insists that granting foreign countries access to stored data could undermine national security and sovereignty and has put forward its own alternative proposal.[143] Until the Budapest Convention is universally adopted, countries like Russia and China can continue to shelter cyber criminals from prosecution.[144] Additionally, many States that have formally ratified the Budapest Convention have yet to pass new domestic legislation to implement its provisions, while other countries have opted out of various provisions by making reservations.[145] Finally, the Convention provides only vague definitions of several key terms and does not elaborate the elements required for various offenses, leaving such details to

---

Budapest Convention].

139. *Chart of Signatures and Ratifications of Treaty 185—Convention on Cybercrime*, COUNCIL OF EUR. (Apr. 20, 2017), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. The membership count is current as of November 27, 2017.

140. John Kerry, Secretary of State, Remarks at Korea University in Seoul, South Korea, An Open and Secure Internet: We Must Have Both (May 18, 2015), http://www.voanews.com/a/text-of-john-kerrys-remarks-in-seoul-on-open-and-secure-internet/2776139.html.

141. Budapest Convention, *supra* note 140, art. 22(1).

142. *Id.* arts. 24(3), 27(1).

143. *See Russia Prepares New UN Anti-Cybercrime Convention—Report*, RT (Apr. 14, 2017), http://www.rt.com/politics/384728-russia-has-prepared-new-international. The Russian Foreign Ministry prepared its own draft convention, which it presented to U.N. experts in April 2017. The Russian draft convention proposes certain forms of international cooperation but contains a special paragraph on the protection of national sovereignty, which critics see as part of Russia's attempt to tighten State control over the Internet. *See id.*

144. *See* SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 210 (2010).

145. Nancy E. Marion, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, 4 INT'L J. CYBER CRIMINOLOGY 699, 703, 705 (2010).

State discretion.[146] As a result, notwithstanding the promise of legal harmonization, inconsistencies in cybercrime legislation and enforcement remain.

Several features of the Convention have also proven controversial. First, there is no dual criminality provision, meaning that activity does not have to be illegal in both the State requesting foreign cooperation and the State whose assistance is requested. A State could therefore be required to investigate acts it considers legal.[147] Second, the Convention requires signatory States to have broad surveillance powers. Article 21 provides that States should collect or record—or compel an Internet Service Provider to collect or record—real-time traffic data associated with online communications,[148] while Article 32 allows law enforcement in one member State to conduct an extraterritorial investigation in another State without notifying that State's authorities.[149] A few commentators have argued that the Convention does not go far enough in authorizing data collection and sharing among States. For example, the Convention does not authorize unilateral cross-border searches, even in emergency situations, instead requiring that nations consult with local officials before seizing data.[150] Many other commentators and civil liberties groups, however, have raised privacy concerns, objecting to the fact that the Convention incorporates the United States' lesser privacy protections rather than Europe's higher standards of data protection.[151]

Concerns about individual privacy may represent the biggest obstacle to the development of a true transnational criminal law of cyber and to the deep international law enforcement cooperation on which national prosecutions often depend. When it comes to the Budapest Convention, though, concerns about privacy may be overblown. Article 15 of the Budapest Convention explicitly provides that each Party shall ensure that the implementation of the Convention is subject to the safeguards provided under its domestic law and respects human rights and liberties.[152] The Convention also does not prevent member States from submitting to stricter privacy standards, like those found in the Council of Europe's Data Protection Convention.[153]

Moreover, from a U.S. perspective at least, international cooperation

146. *See, e.g.*, Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 J. HIGH TECH. L. 101, 113 (2003).

147. Marion, *supra* note 145, at 704.

148. Budapest Convention, *supra* note 138, art. 21(1).

149. *Id.* art. 32(b) ("A Party may, without the authorisation of another Party . . . access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.").

150. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 166-67 (2006).

151. *See, e.g.*, Marion, *supra* note 145, at 705; Brenner, *supra* note 42, at 215; Jonathan Clough, *A World of Difference: The Budapest* Convention on Cybercrime *and the Challenges of Harmonization*, 40 MONASH U. L. REV. 698, 711 (2014).

152. Budapest Convention, *supra* note 138, art. 15.

153. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, ETS No. 108 (Jan 28, 1981), http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

could potentially promote rather than undermine respect for individual privacy. Perpetrators of transnational cyber offenses do not have a reasonable expectation of privacy in malware; code and other information knowingly exposed to the public or shared widely with third parties are not protected under the Fourth Amendment,[154] nor are communications that have been received by the intended recipient.[155] Physical hard drives and server data, though, may be protected by the Fourth Amendment. Currently, under the exigent circumstances exception to the warrant requirement, law enforcement can lawfully search electronic evidence that is in imminent danger of destruction. Given concerns about data being perishable—for example, if it is overwritten or if a device is set to delete information after a certain amount of time—law enforcement may be more likely to rely on the exigent circumstances exception to avoid the warrant requirement.[156] But if police can rely on other countries to effectuate cross-border preservation requests in accordance with the Budapest Convention, they may be less likely to resort to the exigent circumstances exception.

Conversely, if the U.S. government cannot rely on obtaining information relevant to an ongoing investigation from other countries, it may be more likely to try to obtain more data across the board and to retain that data for indefinite periods.[157] Thus, rather than enabling law enforcement to evade Fourth Amendment privacy protections for U.S. residents by relying on other countries, international cooperation on cyber investigations could in fact empower law enforcement to seek appropriate permissions before searching private electronic devices or data. Furthermore, when assessing the privacy risks associated with international cooperation, countries should also factor in the privacy risks associated with the threat of more frequent cyber attacks. If cyber attackers can hack into computers and access files with impunity, allowing law enforcement to collect, review, and share data subject to strict procedural rules may be preferable.

In sum, the Budapest Convention and other efforts to promote international cooperation on cybercrime legislation, investigation, and prosecution are promising, insofar as they recognize that cyber threats often cannot be solved by individual countries acting alone. Ultimately, the Convention's proposals, such as requiring countries to assist with national

154. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." (citations omitted)).

155. *See, e.g.*, United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (holding that a sender's expectation of privacy in a letter "terminates upon delivery").

156. Law enforcement can also obtain consent to electronic searches from infrastructure providers that own computer equipment relevant to an investigation. *See* United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that any third party that has joint access or control over premises or effects can consent to a search even if an absent co-user objects).

157. Recently, the Second Circuit suggested that such overseizure and retention of digital files may be permissible under the Fourth Amendment. *See* United States v. Johnson, 824 F.3d 199, 211-15 (2d Cir. 2016) (en banc) (distinguishing digital files from files in a filing cabinet and observing that the "interspersion [of digital files] throughout a digital storage medium . . . may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data").

investigations and prosecutions, are largely traditional. By preserving the "localized, decentralized system of law enforcement we have had for centuries," the Budapest Convention may not be able to meet the challenge of punishing and reining in transnational cyber offenses.[158] However, if more countries continue to ratify the Budapest Convention, if concerns about privacy can be overcome, and if transnational norm entrepreneurs support States in implementing and complying with the Convention's provisions, the first major international cybercrime treaty may yet prove to be an important instrument for fighting cybercrime. Further, as technology evolves, new protocols can be added to the Convention to strengthen its effectiveness: for example, the Cloud Evidence Group is currently preparing an additional protocol on access for criminal justice purposes to evidence stored on file servers in the cloud.[159] Given the traction that the Budapest Convention has already gained, engaging in diplomatic efforts to bring in new stakeholders and entertaining compromises on certain human rights provisions may be the best way to harmonize the international regulatory environment and to promote accountability through transnational criminal law.

C. International Criminal Law

While legal harmonization and international cooperation could facilitate criminal enforcement at the national level, international criminal law offers another possible accountability mechanism. Prosecution of cybercrimes as international offenses could take place before the International Criminal Court (ICC), or before a sui generis international criminal tribunal for cyber offenses.

Presently, the ICC probably does not have subject-matter jurisdiction over cyber crimes. The Rome Statute establishes the jurisdiction of the ICC over four crimes—the crime of genocide, crimes against humanity, war crimes, and crimes of aggression.[160] Cyber offenses are not specifically recognized anywhere in the Rome Statute and likely do not fit any of the categories of crimes the ICC can hear.

Some commentators have suggested that cyber attacks could constitute crimes of aggression.[161] As originally drafted, the Rome Statute listed the crime of aggression in Article 5 as one of the four crimes over which the ICC had jurisdiction but did not provide a definition of the crime that would enable prosecutions.[162] After the Rome Statute entered into force in 2002, the States

158. THE HISTORY OF INFORMATION SECURITY: A HANDBOOK 717 (Karl de Leeuw & Jan Bergstra eds., 2007).

159. Cloud Evidence Grp., *Cybercrime: Towards a Protocol on Evidence in the Cloud*, COUNCIL OF EUR. (June 8, 2017), http://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud.

160. Rome Statute of the International Criminal Court art. 5(1), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

161. *See, e.g.*, Chance Cammack, *The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression*, 20 TUL. J. INT'L & COMP. L. 303 (2011).

162. *See* Rome Statute, *supra* note 160, art. 5(2) ("The Court shall exercise jurisdiction over the crime of aggression once a provision is adopted in accordance with articles 121 and 123 defining the

parties established a Special Working Group on the Crime of Aggression, charged with drafting a definition of the crime and setting out the conditions under which the ICC would exercise jurisdiction.[163] At a conference in Kampala in 2010, the States parties adopted a definition and jurisdictional regime for the crime of aggression.[164] Since then, thirty-four States have ratified or accepted the Kampala amendments.[165] States parties must additionally activate the Court's jurisdiction over crimes of aggression by a two-thirds majority.[166]

Even assuming the ICC's jurisdiction is activated for crimes of aggression, the definition of the crime of aggression in the Rome Statute amendment is limited to persons "in a position effectively to exercise control over or to direct the political or military action of a State."[167] By limiting potential culpability to those with direct political or military control, the so-called "leadership clause" excludes most perpetrators of transnational cyber offenses. Cyber offenses rarely occur in the context of a strict chain of command; most are carried out "by individuals with only tenuous affiliations to a collective,"[168] and those collectives may or may not be affiliated with, or sponsored by, a State. At least one commentator has suggested that, in exceptional cases, a DDoS attack may meet the leadership clause requirements insofar as the attacker effectively controls the *victim* State, such as when Russian DDoS attackers crippled the Georgian government's ability to act or to communicate with its own people.[169] Still, in most cases, limiting ICC jurisdiction to high-level State actors prevents regulation even of cyber offenses with major international repercussions.

An additional challenge for prosecuting cybercrimes as crimes of aggression is the list of acts of aggression provided in Article 8 *bis* of the Rome Statute, adopted at Kampala.[170] Those actions include an armed invasion, bombardment, and blockade by the traditional armed forces of another State.

---

crime and setting out the conditions under which the Court shall exercise jurisdiction with respect to this crime.").

163. *See* Stefan Barriga, *Against the Odds: The Results of the Special Working Group on the Crime of Aggression*, *in* THE PRINCETON PROCESS ON THE CRIME OF AGGRESSION: MATERIALS OF THE SPECIAL WORKING GROUP ON THE CRIME OF AGGRESSION, 2003-2009, at 1 (Stefan Barriga et al. eds., 2009).

164. *See generally* Claus Kress & Leonie von Holtzendorff, *The Kampala Compromise on the Crime of Aggression*, 8 J. INT'L CRIM. JUST. 1179 (2010).

165. *Amendments on the Crime of Aggression to the Rome Statute of the International Criminal Court*, U.N. TREATY COLLECTION, http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18. The count is current as of November 28, 2017.

166. Rome Statute, *supra* note 160, art. 15(3)*bis* (providing that jurisdiction over the crime of aggression in situations where the case is referred by a State party or by the Prosecutor *proprio motu* can be activated by "the same majority of States Parties as is required for the adoption of an amendment to the Statute"); *id.* art 15(3)*ter* (providing that jurisdiction over the crime of aggression in situations where the case is referred by the Security Council can be activated by "the same majority of States Parties as is required for the adoption of an amendment to the Statute"); *id.* art. 121(3) (providing that adoption of an amendment requires a two-thirds majority).

167. *See id.* art. 8(1)*bis*.

168. Ophardt, *supra* note 20, ¶ 46.

169. *Id.* ¶ 48.

170. Rome Statute, *supra* note 160, art. 8(2)*bis*.

While the phrasing of the definition suggests that the list is exemplary, rather than exhaustive, it is not clear whether cybercrime could qualify as an act of aggression. The enumerated examples all involve the use of armed force, which transnational cyber offenses typically do not, as noted in Section II.A. Cyber attacks resulting in physical damage could conceivably count as crimes of aggression if the list were understood to be merely illustrative, but standard DDoS attacks that disrupt service and cause even significant economic harm would not qualify.

Another possibility for ICC jurisdiction might be to treat transnational cybercrimes as war crimes. Article 8 of the Rome Statute provides jurisdiction over war crimes and enumerates several categories of war crimes, including grave beaches of the Geneva Conventions and violations of other laws applicable in international armed conflict.[171] Most relevant to the cyber context, war crimes include the "extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly" in violation of the 1949 Geneva Conventions,[172] and attacks on civilian objects that are not military objectives.[173] To the extent a cyber attack destroys, rather than simply interferes with, civilian data and communications, cyber attacks carried out in the context of armed conflict could conceivably rise to the level of war crimes. However, it bears emphasizing that war crimes necessarily entail a breach of international humanitarian law; as the previous Part showed, international humanitarian law does not apply neatly to cyber operations and, insofar as it does, very few cyber operations to date qualify as attacks subject to international humanitarian law. Moreover, Article 22 emphasizes the principle of *nullum crimen sine lege*, according to which a person shall not be criminally liable unless the conduct was clearly criminal. The definition of a crime is to be strictly construed and interpreted in favor of the defendant and is not to be extended by analogy.[174] As a result of this inflexibility, cybercrimes that were not explicitly contemplated in Article 8 would be unlikely to qualify as war crimes.[175] At least as currently drafted, then, the ICC's Rome Statute offers a useful model for prosecuting crimes with international effects but would not likely cover transnational cyber offenses.

The Rome Statute could be amended, however, to expand the jurisdiction of the ICC to cover grave cyber offenses. Another solution would be to create a new international criminal tribunal with specialized competency in computer technology.[176] Along these lines, Stein Schjolberg, a former Norwegian judge and an international expert on cybercrime, has long called for an International Criminal Tribunal for Cyberspace and has published a Draft United Nations

171. *Id.* art. 8(2)(a)-(b).

172. *Id.* art. 8(2)(a)(iv).

173. *Id.* art. 8(2)(b)(ii).

174. *Id.* art. 22.

175. *See* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 212-13 (2006).

176. *See, e.g.*, Stahl, *supra* note 4, at 272 ("At the very least, the existence of an international tribunal with universal jurisdiction over acts of cyberaggression would deter such acts and provide a venue for prosecution where nations otherwise often refuse to prosecute such acts.").

Treaty on an International Criminal Court or Tribunal for Cyberspace.[177]

The availability of an international criminal tribunal, whether the ICC or a specialized tribunal, would mitigate many of the problems of State jurisdiction, including jurisdiction shopping, conflict of laws difficulties, and the challenge of cross-border collaboration on evidence-gathering and enforcement. Recent evidence suggests that international criminal tribunals can deter some criminal activity, particularly by governments and rebel groups seeking legitimacy.[178] Moreover, ICC investigations can expose government corruption and unwillingness to comply with international standards, eventually increasing domestic prosecutions in the intermediate term.[179] Thus, international criminal prosecutions of cyber criminals could help to deter cyber offenses on multiple levels.

International law offers two possible ways an international criminal tribunal could obtain jurisdiction over an alleged perpetrator of a transnational cyber offense: universal jurisdiction and complementarity.

1. Universal Jurisdiction

Universal jurisdiction, recognized for centuries as applicable to piracy offenses, offers one solution to the problems of territorial jurisdiction when it comes to criminal liability.[180] Rooted in "the accused's attack upon the international order as a whole,"[181] universal jurisdiction enables an international criminal tribunal (or the courts of any nation) to claim criminal jurisdiction over an accused, regardless of where the crime occurred. Criminal law typically requires some sort of nexus between the prosecuting State and the offense, such as the offense being committed in that State's territory or by a national of that State. But pirates, considered *hostis humani generis*—an enemy of mankind[182]—could historically be prosecuted wherever they were found. In the modern era, piracy continues to be subject to prosecution by any nation under the United Nations Convention on the Law of the Sea (UNCLOS), as

177. STEIN SCHJOLBERG, THE THIRD PILLAR FOR CYBERSPACE: AN INTERNATIONAL COURT OR TRIBUNAL FOR CYBERSPACE (9th ed. 2014), http://www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf.

178. *See, e.g.*, Hyeran Jo & Beth A. Simmons, *Can the International Criminal Court Deter Atrocity?*, 70 INT'L ORG. 443 (2016); Shanay M. Murdock, The International Criminal Court: An Analysis of the Prevention and Deterrence of Atrocity Crimes (2015) (unpublished manuscript), http://commons.lib.niu.edu/bitstream/handle/10843/16390/INTL%20301%20%26%20401%20-%20ICC%20Capstone%20Paper.pdf.

179. *See* Geoff Dancy & Florencia Montal, Unintended Positive Complementarity: Why International Criminal Court Investigations Increase Domestic Human Rights Prosecutions (2015) (unpublished manuscript), http://www2.tulane.edu/liberal-arts/political-science/upload/Dancy-Montal-IO-2014.pdf.

180. *See* Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 HARV. INT'L L.J. 183, 184 (2004). *Compare* RESTATEMENT (SECOND) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 34 (AM. LAW INST. 1965) (listing piracy as the only universal crime) *with* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 404 (AM. LAW. INST. 1987) (enumerating several universal crimes, including war crimes and genocide).

181. ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 58 (1995) (citation omitted).

182. *See* 3 EDWARD COKE, INSTITUTES ON THE LAWS OF ENGLAND 113 (1797).

well as under customary international law.[183] Cyber criminals, too, might be considered *hostis humani generis*: cyber space can be thought of as the modern-day "high seas" and transnational cyber offenses the equivalent of pirates' indiscriminate acts of depredation.[184]

Scholars often assume that universal jurisdiction for piracy is justified only because no State has jurisdiction over the high seas.[185] However, the Court of Appeals for the D.C. Circuit has held that, as Article § 101(c) of UNCLOS, which criminalizes the facilitation of privacy, does not explicitly mention the high seas, aiding and abetting piracy does not need to take place on the high seas to be illegal under the Convention.[186] Thus, it is not a prerequisite for a finding of universal jurisdiction that the crime take place outside the territorial jurisdiction of any country. As applied to the cyber context, the fact that some countries could have jurisdiction to prosecute a crime should not preclude the application of universal jurisdiction to transnational cyber offenses.

Perhaps a better justification for universal jurisdiction over piracy is that it endangers international trade.[187] Transnational cyber offenses can similarly threaten international trade, such as when DDoS attacks disable access to major commercial websites, or when ransomware attacks threaten the destruction of international corporations' records and files. By the same logic, then, severely disruptive transnational cyber offenses could, like piracy, be subject to universal jurisdiction.[188]

The challenge in applying universal jurisdiction to the cyber context is defining the scope of threats for which universal jurisdiction is authorized. The scope must be defined narrowly enough to prevent countries like Russia and China from taking advantage of universal jurisdiction to shut down online

183. United Nations Convention on the Law of the Sea art. 105, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994). Section 404 of the Restatement of Foreign Relations reflects the consensus of the international community and provides that states can have jurisdiction over "certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 404 (AM. LAW INST. 1987).

184. *See* Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 696, 709 (2007).

185. *See, e.g.*, Eugene Kontorovich, *A Guantanamo on the Sea: The Difficulty of Prosecuting Pirates and Terrorists*, 98 CAL. L. REV. 243, 253 (2010) (stating that "the international law of piracy applies only on the 'high seas'").

186. United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013). *But see id.* at 937 (strongly suggesting that "a facilitative act need not occur on the high seas so long as its *predicate offense has*" (emphasis added)).

187. *See, e.g.*, United States v. Yousef, 327 F.3d 56, 104 (2d Cir. 2003) (citing "the threat that piracy poses to orderly transport and commerce between nations" as a basis for universal jurisdiction for piracy); Yvonne M. Dutton, *Bringing Pirates to Justice: The Case for Including Piracy Within the Jurisdiction of the International Criminal Court*, 11 CHI. J. INT'L L. 197, 204 (2010) ("It is the general heinousness of piratical acts and the fact that they are directed against ships and persons of many nationalities—disrupting international trade and commerce—that warrants universal jurisdiction.").

188. *See, e.g.*, Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 116 (2010) ("The application of universal jurisdiction to cyberterrorism fits within the natural evolution of international criminal law and is a logical and measured response to the threat to international peace and security posed by cyberterrorism.").

dissent. If the crimes subject to universal jurisdiction could be carefully drawn, an international criminal tribunal empowered to hear cases against and ultimately sentence cyber criminals anywhere in the world could prove a powerful deterrence mechanism.

2. *Complementarity*

A second basis for jurisdiction over international crimes is complementarity, upon which the ICC relies. Under the complementarity principle, domestic courts retain priority in the exercise of jurisdiction; the ICC may only assert jurisdiction if a domestic court has not already investigated or prosecuted the case.[189] In this way, complementarity is respectful of State sovereignty and may make States more likely to join an agreement like the Rome Statute because they can retain control over matters of importance to them.

Applying the complementarity principle to the prosecution of cybercrimes before the ICC solves some, but not all, of the problems of territorial jurisdiction. If a country proved unable, perhaps for lack of technical capacity, or unwilling to prosecute a case domestically, the case could potentially be tried before the ICC. A time limit would have to be established within which the State would be required to commence a prosecution, if it so chose; if a State failed to take action during that time, a victim State could request that the Prosecutor of the ICC press charges. Thus, the availability of an international criminal tribunal with jurisdiction to hear cases involving grave harm to any member State would solve the problem of States being unwilling to prosecute or extradite their nationals. Complementarity may also incentivize countries to adopt and enforce legislation criminalizing transnational cyber offenses in order to keep cases in their own courts. At the same time, complementarity fails to address some of the problems of territorial jurisdiction, including the risk of an Internet actor being subject to the potentially differing laws of many different countries, without having meaningfully consented to the jurisdiction of those countries.

Even if victim States wanted the ICC to exercise jurisdiction, the ICC's jurisdiction is largely limited to ratifying States, which can refer cases to the ICC if the alleged crime is committed by a national of, or on the territory of, that State.[190] Precisely what it would mean for a cybercrime to be committed on a State's territory is not clear. Taking a very broad view of ICC jurisdiction, according to which the physical routing of attacks would determine whether a State party to the Rome Statute was the site of a crime,[191] both the primary State victim and the State whose infrastructure was exploited could provide the jurisdictional hook. Since transnational cyber offenses are often routed through

189. Rome Statute, *supra* note 160, pmbl. & arts. 1, 15, 17-19.

190. *Id.* art. 12. In addition to jurisdiction over the nationals of a State party or over crimes committed on the territory of a State party, the ICC can also exercise jurisdiction over any individual when the Security Council refers a case to the Prosecutor under Chapter VII of the Charter of the United Nations. *Id.* art. 13(b).

191. *See* Ophardt, *supra* note 20, ¶ 74.

a large number of territories,[192] the jurisdictional bar could often be overcome. But taking a narrower view of jurisdiction, crimes with a merely incidental relationship to a country would not qualify as a crime committed on that country's territory. Finally, even if the ICC could properly exercise jurisdiction over a defendant who was not a national of a member State, it could face the same extradition problems described above.

Clearly, there are significant challenges to prosecuting cyber criminals under international criminal law.[193] However, international criminal tribunals are a still-recent development, and a new tribunal could potentially be created to hear cases of cyberterrorism and other serious cybercrimes that threaten governmental institutions, cause large economic losses, or substantially interfere with civilian Internet usage. Were such a tribunal to exist, it would send a powerful message to the online community and could go a long way towards ending impunity.

CONCLUSION

In the absence of viable tools to hold cyber attackers responsible, individuals, States, and businesses may be tempted to resort to retaliation and cyber-vigilantism. While scholars have long recognized the need for accountability for cyber wrongs, there has been little agreement as to what legal framework for accountability is most appropriate. The very fact that experts have struggled to settle on an appropriate legal framework suggests that there is no single legal framework that can properly regulate all cyber hostilities. In the cyber realm, we may encounter conventional crimes properly subject to domestic criminal law as well as violations that fall under the international law of armed conflict. Critically, however, the cyber context also gives rise to a third category of wrongs that do not fit comfortably within either domestic criminal law or the law of armed conflict: transnational cyber offenses.

The jurisdictional rules developed for the nineteenth-century world of Westphalian nation-states are in many ways at odds with the network architecture of modern computing and the inherently cross-border character of transnational cyber offenses. Regulation and deterrence of transnational cyber offenses require novel legal solutions. While the elaboration and implementation of those solutions may seem like a formidable challenge, there is reason to be cautiously optimistic. Transnational cyber offenses, unlike many acts that the international community has sought to condemn, harm all countries; *no* country is immune from the threat of cyber hostilities. The WannaCry ransomware attack, to give just one recent example, made clear that even supposed cybercrime havens like Russia may find themselves victims of

192. *Id.* ¶ 57.

193. *See, e.g.*, Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1, 7, 35-37 (2010) (explaining that cyberterrorism—"the use of computer networks in order to harm human life or to sabotage critical national infrastructure in a way that may cause harm to human life"—is not covered by any of the four crimes over which the ICC has jurisdiction).

transnational cyber offenses. As Internet-connected devices proliferate and the security risks multiply, countries may face both internal and external pressures to develop and enforce a comprehensive international accountability regime—to form, as Barlow himself alluded to, a "Social Contract" of the digital world.[194]

194. Barlow, *supra* note 1.

THE YALE JOURNAL OF INTERNATIONAL LAW

Many of the social arrangements we think of as quintessentially domestic . . . are inextricably interwoven with complex processes in other countries and regions of the globe. Consider: our security system; our political-economic system; the search to find and retain external markets for our products; our dependence on the natural resources without which an advanced industrial and science-based civilization cannot survive; our health system; our conceptions of fundamental morality . . . . Even "domestic law" courses can no longer be understood adequately—whether for descriptive or practical professional purposes—without an understanding of the organization and dynamics of the international system.

—W. Michael Reisman

The Yale Journal of International Law (*YJIL*), now in its forty-third year, is a primary forum for the discussion and analysis of contemporary international legal problems. Published twice a year at the Yale Law School, *YJIL* contains articles, notes, comments, and book reviews written by top international scholars, practitioners, and students.

Recent issues have featured discussions of a wide array of international legal, political, social, and economic issues, including: U.S. engagement with international human rights bodies; the standard of review in investor-state arbitrations; the international obligation to protect trademarks; the recognition of cultural property rights; enforced disappearance under international law; and the crime of aggression.

Our authors have included José E. Alvarez, Lea Brilmayer, Vahakn N. Dadrian, Owen Fiss, Oona Hathaway, Harold Hongju Koh, David Luban, W. Michael Reisman, Peter Schuck, Gregory Shaffer, Theodore Sorensen, and William H. Taft IV. Don't miss important discussions of crucial global issues—subscribe to *YJIL* today.

THE YALE JOURNAL OF INTERNATIONAL LAW
Yale Law School
P.O. Box 208215
New Haven, CT 06520-8215

Please enter my one-year subscription to *The Yale Journal of International Law*.

Name

Address

City State Zip Country

❑ $38.00 for one year (domestic) ❑ $48.00 for one year (foreign)

Order must be accompanied by payment.

Checks should be made payable to The Yale Journal of International Law.

The editors would like to acknowledge, with gratitude, the generous support for the *Yale Journal of International Law* in its forty-third year from:

CHARLES L. FELSENTHAL
THE FELSENTHAL DONATION IN MEMORY OF HARRY D. FELSENTHAL
W. MICHAEL REISMAN
NICHOLAS ROSTOW
THE ROSTOW DONATION IN MEMORY OF EUGENE V. ROSTOW

The editors would also like to recognize the thoughtful contributions of:

LEA BRILMAYER
HEATHER K. GERKEN
PAUL GEWIRTZ
OONA A. HATHAWAY
HAROLD HONGJU KOH
W. MICHAEL REISMAN
KEVIN ROSE
SUSAN ROSE-ACKERMAN
MIKE K. THOMPSON
THE YJIL ADVISORY BOARD