May 15, 2017

A "PROBLEM WITHOUT A PASSPORT"[1]: OVERCOMING JURISDICTIONAL CHALLENGES FOR TRANSNATIONAL CYBER AGGRESSIONS

Alexandra Perloff-Giles

Introduction

Just over twenty years ago, John Perry Barlow issued his "Declaration of the Independence of Cyber Space." In it, he offered a vision of 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 does not lie within your borders.[2]

Whereas once national political authorities could control the circulation of information, in the digital age information flows freely throughout the world. The Internet exists "both everywhere and nowhere."[3]

---

[1] Kofi Annan used the term "problems without passports" to refer to challenges like environmental threats that transcend borders and that cannot be addressed by any one nation alone. *See, e.g.*, 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).

[2] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

[3] *Id*. Of course, the infrastructure of the Internet is physical. As international security expert Robert Axelrod explained: "[E]very node of the network, every router, every switch is within the sovereign borders of a nation-state and therefore subject to its laws or travels on a submarine cable or satellite connection owned by a company that is incorporated in a sovereign nation-state and therefore subject to its laws. In other words, there is no non-sovereign, 'free' part of cyberspace." P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 182 (2014) (quoting a September 5, 2011 e-mail message from Robert Axelrod to the authors). But the ability to hide one's physical location,

The scale and global reach of the modern Internet, coupled with the low cost of launching a cyber attack, have led to the proliferation of cyber threats.[4] As one former FBI official described the current situation, "[t]he accessibility of the information infrastructure, global connectivity and the rapid growth of a computer-literate population combine to ensure that millions of people around the world possess the means to engage in a cyber attack simply by downloading an automated hacking tool from a website."[5]

Barlow's founding vision of a borderless, decentralized, extra-governmental Internet—and the contemporary reality of widespread hacking with potentially global repercussions—are at odds with a territorial jurisdiction model centered on the nation-state.[6] Indeed, David Johnson and David Post argued early on that geography-based regulation was inadequate for regulating the Internet, since "there

---

the speed with which data travels, and other features of the Internet make those sovereign borders less meaningful.

[4] As used here, "cyber attacks" includes any cyber operations that cause damage, disruption, or destruction. I in no way mean to suggest that these attacks would constitute "armed attacks" that would justify the resort to self-defense under Article 51 of the U.N. Charter, nor that they would necessarily be subject to the prohibitions and restrictions on military attacks under international humanitarian law.

[5] Prepared Statement of Michael A. Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, Hearing Before the Joint Economic Committee Congress of the United States, Cybercrime, Transnational Crime and Intellectual Property Theft, S. Hrg. 105-489 (Mar. 24, 1998).

[6] Internet governance expert Milton Mueller has described five ways in which the Internet is at odds with the nation-state: it "globalizes the scope of communication," making "borderless communication the default;" (2) it dramatically expands the scale of communication, with a "sheer volume of transactions" that "often overwhelms the capacity of traditional governmental processes to respond; (3) it "distributes control," "ensur[ing] that the decision-making units over network operations are no longer closely assigned with political units"; (4) it spawned new transnational institutions like the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN); and (5) it facilitates "radically new forms of collaboration, discourse, and organization." MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 4 (2010)

is no geographically localized set of constituents with a stronger and more legitimate claim to regulate" the Web than any other state.[7] How, then, to address the proliferation of cyber threats, given the limitations of a territorial jurisdiction system?

That question animates this paper. In Part I, I review the history of the Internet, with particular attention to architectural features that were designed for survivability rather than security and that facilitate the rapid dissemination of cyber attacks across borders. I describe the ways in which some of the most common cyber attacks operate, and define a new category of cyber attack—what I call "transnational cyber aggressions"—that pose a singular challenge to the territorial model of jurisdiction. In Part II, I explain *why* transnational cyber aggressions in particular cannot be adequately regulated under the standard legal frameworks of crime or war. Reassessing the much-debated issue of whether existing law applies to cyber, 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 aggressions.[8] In Part III, I offer three case studies—the Love Bug virus; the 2007 cyber attacks on Estonia;

---

[7] David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996).

[8] 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 1 (1956). Cyber activities are perhaps the quintessential example of transnational events.

and the very recent ransomware attack—to illustrate the unique challenges of regulating transnational cyber aggressions. The inadequacy of ordinary domestic criminal law in addressing cases like these highlights the need for new regulatory solutions for transnational cyber activity.

Finally, in Part IV, I propose possible legal solutions for perpetrators of transnational cyber aggressions 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 resolution to offer novel solutions based on international civil arbitration, transnational criminal law, and international criminal law. While this paper does not presume to have definitive answers, I hope it inspires other scholars to look beyond the traditional legal paradigms and consider what role international institutions might play. As the number of transnational cyber aggressions continues to escalate, and the nascent Internet of Things 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 Attack

a. Historical Overview of Internet Design

The same features of the Internet crafted to ensure its survivability in the Cold War era create vulnerabilities today. Data makes many short trips as it travels through computer networks, rather than along a single, consistent pathway. The node network system opens up many more points of attack and allows attacks to spread widely, across geographic boundaries. Put briefly, "the origin of the threat posed by cyberspace is found in the architecture of the Internet itself."[9] For that reason, a short account of the history and design of the Internet will help to shed light on contemporary cyber attack methods.

In the early 1960s, as the United States and the Soviet Union were building up their nuclear ballistic missile systems and 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."[10] Consequently, American officials and researchers sought alternatives to command and control communications systems that could withstand nuclear devastation.

---

[9] 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).

[10] JANET ABBATE, INVENTING THE INTERNET 16 (1999) (quoting PAUL BARAN, ON DISTRIBUTED COMMUNICATIONS V (1964)).

Taking up that challenge, Paul Baran, an engineer at RAND, developed a new communications network built around the principles of redundancy and decentralization. In contrast to telephony systems, Baran's system relied on a distributed network, whereby each node was connected to multiple other nodes in a web. Information would be routed from one node to another until it reached its final destination in a process Baran referred to as "hot-potato routing."[11] Without a centralized switching facility, links could survive attacks on some of the switching nodes: if there was a problem or congestion at one node, information could 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."[12] Compared to hierarchical systems, Baran's distributed network had the advantage, as he described it, of "survivability . . . in the cases of enemy attacks directed against nodes, links, or combinations of nodes and links."[13]

---

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

[12] Paul Baran, *On Distributed Communications Networks*, 12 IEEE TRANSACTIONS ON COMMUNICATIONS 1, 8 (1990). The distributed network, made up of many short links connected by nodes, was made possible by the emergence of digital technology. Analog signals 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 10, at 16.

[13] Nick Schulz, *The "Myth" of the Invention of the Internet*, AM. ENTERPRISE INST. (July 13, 2012, 1:02PM), http://www.aei.org/publication/the-myth-of-the-invention-of-the-internet; *see also* ABBATE, *supra* note 10, at 10 (quoting an interview with Baran in which he explained that "[b]oth the US and USSR were building hair-trigger nuclear ballistic missile systems. . . . If the strategic weapons command and control systems could be more survivable, then the country's retaliatory capability could better allow it to withstand an attack and still function.").

Additionally, Baran's system divided information into packets, or what he termed "message blocks."[14] 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 message into packets had the advantage of making it more difficult for spies to eavesdrop.[15]

Baran's research proved influential to the development of ARPANET, a network funded by the U.S. Department of Defense's Advanced Research Projects Agency.[16] ARPANET initially consisted of four "gateway computers" called Interface Message Processors (IMPs) that determined how to route packets based on the quality of the connection to neighboring IMPs; each IMP made independent routing decisions to decide the next step of the packet's journey. As more computers got added to the network, design specifications developed to ensure continued interoperability of the IMPs. Thus, routing protocol implementation combined decentralized decision-making at each gateway with elements of centralized ARPANET control.[17]

---

[14] Education and Technology History Wiki, Interview by David Hochfelder with Paul Baran (Oct. 24, 1999), http://ethw.org/Oral-History:Paul_Baran
[15] ABBATE, *supra* note 10, at 19.
[16] Ashwin J. Mathew, *The Myth of the Decentralised Internet*, 5 INTERNET POL'Y REV. 1 (Sept. 30, 2016), http://policyreview.info/articles/analysis/myth-decentralised-internet.
[17] *Id*.

As ARPANET grew, network operators realized that a single network would become unmanageable and decided to create a "network of networks" that could communicate with one another. ARPANET's successor, NSFNET (funded by the National Science Foundation), adopted a "three-tiered hierarchical network topology": the NSF backbone network connected broad regional networks, which in turn connected networks within more circumscribed geographical regions.[18] The Policy Routing Database, a database of routing information maintained by the operators of the NSFNET backbone, recorded the addition of new regional networks to the NSFNET and allocated Internet Protocol (IP) address space. Security was of minimal concern; according to members of the research community that developed and operated NSFNET, "everybody trusted everybody."[19]

The World Wide Web, invented in 1989, progressed rapidly in the early 1990s, making the Internet easier to navigate and spurring commercial interest. In 1995, the U.S. government relinquished control over the Internet, bringing an end to the three-tiered hierarchical structure of NSFNET and giving rise to a complex network topology. The founders of the modern Web embraced an ethos of openness and aspired to a model of "radically democratic"[20] social organization rather than governmental or corporate control. Today, the topology of the Internet routing system consists of over 55,000 individual networks, situated within dozens of large

[18] *Id*.
[19] *Id*.
[20] Jennifer Stisa Granick, *The Death of the Internet Dream*, BACKCHANNEL (Aug. 17, 2015), http://medium.com/backchannel/the-end-of-the-internet-dream-ba060b17da61.

networks that control routing and that extend across geographic borders.[21] 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. The advent of cloud computing, which is intrinsically global, further accentuates the tension between the national sovereignty and the borderless nature of online activity.

As this history shows, the modern Internet reflects a deliberate repudiation of centralized, top-down authority. How, then, to address threats and to design regulatory systems for a technological landscape that was designed to prioritize survivability and flexibility over security, that is open and accessible to anyone, and that lies outside the exclusive control of any single authority or jurisdiction?

b. Cyber Attack Methods

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. What they failed to consider, however, was the possibility of damage caused by the very data being communicated.[22] Several kinds of cyber attacks can be carried out through code. Some are direct attacks by a single

---

[21] *Id*.

[22] *See, e.g.*, Stahl, *supra* note 9, 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 it transfers."); *see also* ABBATE, *supra* note 10, at 5 (1999) (claiming that ARPANET "favored military values, such as survivability, flexibility, and high performance").

perpetrator against a single victim—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. Direct attacks that affect only a particular target replicate the kinds of attacks that exist in the kinetic world: a thief can steal the credit card of an unsuspecting victim; a corporate spy can sneak in and obtain trade secrets; a government can bomb or otherwise disable another country's nuclear weapons facility. Other kinds of cyber attacks are indirect. Less targeted and more readily transmitted, indirect attacks can be considered the quintessential *cyber* attacks: they exploit the decentralized, networked nature of the Internet to cause harms that have no kinetic-world equivalent.

Infectious malware and denial-of-service are two common examples of indirect cyber attacks. 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, both spread easily from one computer to another. Viruses insert themselves into an executable file or program, laying dormant until a user runs the infected program, and then getting 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 use features of the cyber world, whether interoperability or Internet connectivity, to disseminate threats to potentially unknown victims.

A second common indirect cyber attack 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, and occasionally even days.[23] The use of zombie armies or botnets enables hackers to execute attacks "across many different, geographically dispersed computer servers" rather than from "a single point of command."[24] For example, the October 2016 DDoS attack on US-based data centers caused ripple effects not only across the United States but also in Europe.[25] In many cases, the attacker can

[23] DDoS attacks can take place either at the application layer (Layer 7), or at the network 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 layer attacks send malicious requests over different network protocols, consuming all available bandwidth and shutting down most network infrastructures.

[24] SUSAN W. BRENNER, CYBERTHREATS 2 (2009).

[25] On October 21, 2016, 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. A hacker group called New World Hackers, comprising members from Russia and China and perhaps elsewhere, took responsibility for the attack. The FBI and the Department of Homeland Security are currently conducting an investigation. *See* Tess Owen, *What You Need To Know About Friday's Massive Cyber Attack*,

remotely control zombie devices without the device owner even knowing their device has been 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.[26]

At the dawn of the Internet of Things, DDoS attacks are poised to become an even bigger threat. As more and more ordinary devices, from thermostats to coffee pots, become connected to the Internet and use standardized operating systems, not only are there more potential targets for attackers, but also the potential size and force of zombie botnets increases.[27]

As these examples of indirect cyber attack methods demonstrate, the Internet gives rise to new kinds of threats that get propagated through cyberspace. The architectural interconnectivity of the Internet, as it has developed, creates "collective vulnerability."[28] 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, the challenge becomes not just how to respond but who has the jurisdiction to do so and whether they can hold perpetrators accountable.

VICE NEWS (Oct. 23, 2016), https://news.vice.com/story/what-you-need-to-know-about-fridays-massive-cyber-attack.

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

[27] Symantec, *IoT Devices Being Increasingly Used for DDoS Attacks* (Sept. 22, 2016), http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

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

c. Transnational Cyber Aggressions Defined

The cyber attacks described above are examples of what I call "transnational cyber aggressions." In attempting to situate cyber activities within either the criminal law or the law of war framework, experts have paid little attention to the distinctive features of *transnational* cyber aggressions, despite the fact that *most* cyber attacks are transnational.[29] Transnational cyber aggressions ripple across borders, ignoring territorial boundaries and challenging jurisdictional rules. They may be carried out by individuals or non-state groups, affiliated or not with a government, and they may target individuals, corporations, foreign media, state entities, or all of the above. Direct attacks could constitute transnational cyber aggressions if the perpetrator and victim sit in different countries. More often, though, transnational cyber aggressions are indirect attacks, which exploit the global, interconnected architecture of Internet communications as they ricochet and spread from one country to another.

Transnational cyber aggressions implicate multiple jurisdictions for several reasons. First, the Internet makes it easier to instigate cross-border attacks. Attacks can be launched from any location with Internet access, and attackers can readily hide their location with anonymizing services that make "the task of identifying a

[29] Testimony by Jason Weinstein, Criminal Division, U.S. Department of Justice, Before U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, *Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism*, 112th Cong., 1st sess., April 12, 2011, http://www.justice.gov/criminal/pr/testimony/2011/crmtestimony-110412.html.

data user's location exceedingly difficult."[30] Moreover, the Internet reduces the transaction costs of cross-border cooperation in planning and executing attacks.[31]

Second, data transmitted on the Internet ordinarily moves through various jurisdictions, enabling a single piece of malicious code to be routed through multiple countries.[32] Internet traffic, designed to travel through the *fastest* route, may not always take the most geographically *direct* route. And because of the packet system, whereby different packets can take different routes, the potential for information to traverse different jurisdictions is multiplied.[33] Network architecture makes it difficult to predict for Internet users to predict the territorial jurisdictions of which they are potentially availing themselves:[34] "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."[35]

---

[30] Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 331 (2015).
[31] Kamala D. Harris, Office of the California Attorney General, *Gangs Beyond Borders: California and the Fight Against Transnational Organized Crime* (March 2014), http://oag.ca.gov/sites/all/files/agweb/pdfs/toc/report_2014.pdf, at 59 ("[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.").
[32] *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. 1, 22 (2010).
[33] *Id.* at 11.
[34] Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 56 (2001) ("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.").
[35] Daskal, *supra* note 30, 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.").

Third, as described above, many cyber attacks do not have a single target but rather spread virally, such that the impact of an attack can be felt far from either the launch point or the target first hit.[36] For example, in May 2008, a suspected Chinese cyber attack caused an estimated 50 million people to lose power in both the United States and Canada.[37] In short, the ways in which many cyber attacks originate, move through cyber space, and affect their targets are distinctly transnational. By recognizing transnational cyber aggressions as a distinct category, we can begin to formulate legal solutions that fit the technological realities, instead of trying to fit quintessentially digital problems into standard regulatory frameworks.

II. Beyond Domestic Criminal Law and IHL: Transnational Cyber Aggressions 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)."[38] In the cyber context, we have largely replicated that division: efforts to combat computer crime fall largely to the FBI, while cyberwarfare is within the authority of the Defense Department. But the division becomes

---

[36] Kristin M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CONG. RES. SERV. (Jan. 17, 2013), at 5 ("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.").

[37] David Gewirtz, *Digital Defense: The Coming Cyberwar*, 14 J. COUNTERTERRORISM & HOMELAND SECURITY INT'L 48, 49 (2008).

[38] Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 207, 209 (Jack M. Balkin et al., 2007).

complicated in the cyber context where, as Susan Brenner has pointed out, "what we define as 'internal' threats can now come from external, civilian actors."[39]

The bulk of the scholarly literature on cyber threats has similarly been wed 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. A few scholars have explored both domestic criminal law and the law of armed conflict in an effort to determine what body of law is most appropriate to address cyber conflicts.[40] But very rarely do authors look outside of the traditional dichotomy. Rather than attempt to apply any one existing legal framework to all cyber threats, this paper contends that we ought to be more attentive to the particular characteristics of the cyber threat. Just as there is no single body of law for all wrongful acts in the physical world, so too is there 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 analogs in the kinetic world, such as child pornography or financial fraud, domestic criminal law is generally appropriate. Where the perpetrator of such crimes is located in the same jurisdiction as the victim, prosecution is relatively straightforward. For other kinds of cyber hostilities—namely, destructive attacks by one government against another government—the law of armed conflict offers an appropriate legal framework. The

---

[39] *Id.*

[40] *See, e.g.*, Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 817 (2012).

Stuxnet attack, for example—one of the most dramatic and damaging cyber events to date—can be analyzed in *jus ad bellum* terms: it involved an act of aggression by states (the United States and Israel) against another state (Iran), and, according to some scholars at least, it rose to the level of an Article 51 armed attack.[41] But the law of war provides a useful framework for only a "very small number" of cyber attacks.[42]

Transnational cyber aggressions, however, do not fit comfortably in either category.[43] 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 the civilian information infrastructure do not look like traditional warfare between states. Transnational cyber aggressions are undertaken by private individuals or non-state groups, not states,[44] and to the extent they could be attributed to national governments, few such incidents constitute a "use of force"

---

[41] *Tallinn Manual on the International Law Applicable to Cyber Warfare* 57-58 (Michael N Schmitt ed., 2013) (noting disagreement among the Tallinn Manual drafters on whether Stuxnet represented an armed attack).

[42] Hathaway et al., *supra* note 40, at 817.

[43] Because neither domestic criminal law nor the laws of war are appropriate to such attacks, it is not clear what governmental institution bears responsibility for taking action in response to such attacks. The Department of Justice, the FBI's Cyber Division, the Department of Homeland Security, the Department of Defense, the US Army's Cyber Command (CYCOM), and the Office of the Director of National Intelligence all have roles to play in cyber threat response in the United States. In July 2016, the Obama Administration released Presidential Policy Directive 41 on cyber incident coordination, which details the "architecture of federal government response coordination for significant cyber incidents." White House, Presidential Policy Directive/PPD-41, United States Cyber Incident Coordination (July 26, 2016), http://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

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

under Article 2(4) of the United Nations Charter.[45] Transnational cyber aggressions 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 two traditional legal frameworks and their limitations when it comes to the regulation of transnational cyber aggressions.

a. The International Humanitarian Law Framework and Its Limitations

International law offers potentially useful guidance for addressing cyber aggressions 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 United Nations Declaration of Human Rights or the International Covenant on Civil and Political Rights 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 news media.

More often, though, international law approaches to cyber aggressions have focused on the law of armed conflict. The law of armed conflict, codified notably in the post-war Geneva Conventions and their Additional Protocols, was designed to regulate traditional horizontal warfare between nation-states. Under the two-part test elaborated by the International Tribunal for the Former Yugoslavia in the celebrated *Tadíc* case, in order for a conflict to qualify as an armed conflict, armed groups must satisfy the requisite degree of organization, and armed confrontations

[45] U.N. Charter art. 2, ¶ 4.

must meet the requisite level of intensity.[46] Where the organization and intensity requirements are satisfied, a conflict between two or more states qualifies as an international armed conflict, subjecting the states involved to the Geneva Conventions and Additional Protocol I. Conflicts between organized armed groups, or between a state and an organized armed group, are non-international armed conflicts that are governed primarily by Common Article 3 to the Geneva Conventions and by Additional Protocol II. Since non-international armed conflicts were not the paradigmatic example of conflict when the Geneva Conventions were adopted, there is relatively sparse international law that governs them: non-state actors often operate outside the scope of international humanitarian law, fighting, as Cherif Bassiouni put it, "in a twilight zone between lawful combatancy and common criminality."[47]

Applying international humanitarian law (IHL) principles to cyber conflict raises several questions. First, what does it take for a cyber attack to satisfy the intensity threshold? The International Committee of the Red Cross (ICRC) has taken the position that cyber attacks need only "disable[]" an object to qualify as an armed attack; they need not cause physical damage or destruction.[48] Echoing the ICRC, Michael Schmitt, director of the Tallinn Manual Project, has asserted that, when a cyber attack is attributable to a state and is "either intended to cause injury, death,

---

[46] *Prosecutor v. Tadić*, IT-91-1-T, Trial Chamber Judgment of 7 May 1997.
[47] M. Cherif Bassiouni, *The New Wars and the Crisis of Compliance with the Law of Armed Conflict by Non-State Actors*, 98 J. CRIM. L. & CRIMINOLOGY 711, 725 (2008).
[48] 31st International Conference of the Red Cross and Red Crescent, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (Oct. 2011) Report 31IC/11/5.1.2, at 37.

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."[49] Even if physical destruction is not a strict prerequisite, very few, if any, cyber events to date would qualify as "armed attacks" permitting states to respond with either cyber or kinetic force in self-defense. Cyber attacks targeting government facilities or critical infrastructure such as hospitals or power grids could potentially qualify, but the vast majority of cyber operations lie below the "armed attack" threshold of Article 51.

The second major challenge in applying IHL principles to cyber hostilities is attribution. As the ICRC has noted, "the digitalization on which cyberspace is built ensures anonymity and thus complicates the attribution of conduct."[50] In contrast to traditional warfare, which requires "a group capable of mounting typical military operations," in the cyber context "massive attacks can be launched by a single individual or by a group that is organized entirely online."[51] Even if forensic investigators are able to conclusively determine that an attack emanated from a particular country, it is very difficult to definitively attribute an attack to a foreign government under state responsibility doctrine. Historically, there was little doubt if an attack was carried out by a foreign power: soldiers were uniformed, and only nations had the resources to carry out attacks in another country. Today, however, cyber attacks can be carried out at low cost by states, by hacker groups with ties to

[49] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 IRRC 365, 374 (June 2002).
[50] 31st International Conference, *supra* note 48, at 37.
[51] Michael Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SECURITY L. 245, 246 (2012).

foreign governments, or simply by individuals whose identities and geographic locations are frequently hidden. Thus, attributing responsibility for an attack to a hostile nation 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 logical legal framework. The Stuxnet attack on the Natanz nuclear enrichment facilities—perhaps the most infamous cyber attack to date—is one such example. Stuxnet was a targeted direct attack on a nuclear facility operated by the Iranian government. The attack 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 and few states have the capacity to build and deploy Stuxnet.[52] 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 aggressions.[53] Indeed, buried inside the code was a "do-not-infect" indicator; when the virus encountered a computer that did not fit the target profile, the virus

[52] Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUDIES 4, 22 (2015).

[53] 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." THE HANDBOOK OF THE CRIMINOLOGY OF TERRORISM 555 (Gary LaFree & Joshua D. Freilich, eds. 2016).

destroyed itself, minimizing incidental or "knock-on" effects.[54] The Stuxnet attack thus fits within familiar paradigms of states carrying out targeted, politically-motivated strikes against other states. While determinations of intensity and attribution can be challenging, international humanitarian law provides the right framework for analyzing—and potentially responding to—incidents like Stuxnet. For transnational cyber aggressions, however, where the attacker and the victim are not both nation-states, the international humanitarian law framework is unavailing.

b. The Domestic Criminal Law Framework and Its Limitations

While international humanitarian law governs cyber hostilities between states, domestic law appropriately regulates cyber activities that take place within a single state. Domestic criminal law is a tool for the "protection of public mores within a specific locality"[55]: it functions effectively when the crime takes place in a particular jurisdiction, which is able to regulate the activity, investigate the crime, and punish the perpetrator. In concrete terms, domestic criminal law is generally appropriate for 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.

---

[54] 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.

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

Domestic criminal law is ill-adapted, however, to transnational cyber aggressions, which have effects beyond the reach of a state's police power.[56] Law enforcement agencies are candid about the difficulties of policing crimes that implicate multiple jurisdictions. In his testimony to Congress, FBI Assistant Director Thomas Kubic evoked many of the challenges of the Westphalian nation-state model 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 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.[57]

As Kubic's testimony points up, the transnational nature of many cyber aggressions is at odds with a territorial jurisdiction model. Historically, cross-border activity was rare: territoriality established "the bedrock principle[] for the

---

[56] *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 ("Overlapping and often conflicting territorial criteria make both the application of laws in cyberspace and the resolution of Internet-related disputes difficult and inefficient.")

[57] Thomas T. Kubic, Deputy Assistant Director, FBI, Testimony Before the House Committee on the Judiciary, Subcommittee on Crime (June 12, 2001), http://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

development of modern international law."[58] We may distinguish between three categories of territorial jurisdiction: 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).[59] Transnational cyber aggressions are problematic from all three perspectives.

When it comes to legislative jurisdiction, different countries have different laws governing cybercrime. Online activity could be subject to the laws of multiple jurisdictions, which may overlap or conflict. As Paul Schiff Berman explains, "in an electronically connected world the effects of any given action may immediately be felt elsewhere with no relationship to physical geography at all."[60] 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,[61] 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 subjecting an actor to jurisdiction potentially anywhere in the world[62] would raise a multitude of

[58] KAL RAUSIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 11(2009).
[59] *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (describing categories of jurisdiction).
[60] PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS 92 (2012).
[61] Uta Kohl, *Jurisdiction in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 30, 33 (Nichlas Tsagourias & Russell Buchan eds., 2015).
[62] *See, e.g.*, 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

problems. Indeed, long before the Internet, James Brierly remarked that "[t]he suggestion that every individual is or may be subject to the laws of every State at all times and in all places is intolerable."[63] Among the problems with subjecting Internet users to the laws of every country is the absence of any meaningful consent 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, one is subject to that sovereign nation's laws," but if an individual sends data over the Internet that happens to transit through another nation, "that individual is not consciously choosing to bind himself to any particular foreign government's laws."[64]

Subjecting every online actor to the law of every state, under a theory that activity on the Internet can be felt anywhere, is a flawed solution to the problem of transnational cyber aggressions. 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

---

page could be subject to jurisdiction by all of the nearly three-hundred sovereigns around the world."); 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.").

[63] James L. Brierly, *The "Lotus" Case*, 44 L.Q. REV. 154, 161 (1928).

[64] Daskal, *supra* note 30, at 367-68.

territory—and countries are unlikely to forego jurisdiction over incidents affecting their own citizens.[65]

Even as legislative jurisdiction may be overinclusive in the context of cyber activity, it may also be underinclusive. Laws must apply extraterritorially for a state to bring charges for criminal acts initiated outside its territorial limits. In the absence of extraterritorial application of cybercrime legislation, attackers can jurisdiction shop for favorable jurisdictions where their activities are not proscribed. Most domestic cybercrime laws, including in the United States, do not apply extraterritorially;[66] extraterritorial exercises of authority are typically seen to infringe upon the sovereignty of other countries.[67] 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."[68]

In recent years, though, 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 Alexei Ivanov were found responsible for stealing data and extorting money from American businesses. Since Russia does not extradite its nationals accused of cybercrime, the United States developed a clever

---

[65] *See, e.g.*, Andre R. Jaglom, *Liability On-Line: Choice of Law and Jurisdiction on the Internet, or Who's In Charge Here?*, http://www.thsh.com/documents/liabilityon-line.pdf, at 10.
[66] *See* Hathaway et al., *supra* note 40, 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.").
[67] Anthony J. Colangelo, *What Is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303, 1311-12 (2014).
[68] CLAUDE LOMBOIS, DROIT PENAL INTERNATIONAL 536 (2d ed. 1979).

strategy to overcome the jurisdictional challenges. The government created a fake computer security firm, "Invita," and invited Gorshkov and Ivanov to come to Seattle to interview with the firm. The FBI promptly arrested them both. Gorshkov was tried in Washington and sentenced to three years in jail,[69] while Ivanov's case was transferred to Connecticut,[70] where the district court determined that the 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.[71] But the successful prosecutions of Gorshkov and Ivanov under U.S. law are the exception not the norm. A territorial approach to jurisdiction over transnational cyber aggressions may lead to either too many or too few countries exercising legislative and adjudicative jurisdiction.

A territorial approach to jurisdiction can also be problematic from the point of view of enforcement jurisdiction for two reasons: other countries may be unable to provide the necessary digital evidence or unwilling to cooperate with investigations and extradition. First, enforcing cybercrimes requires expertise and resources that not all states have. As Abraham Sofaer and Seymour Goodman note, "[a] great disparity exists . . . in the legal and technological capacity of states to meet

---

[69] *See* United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (finding that law enforcement was justified in downloading data from a Russian computer without a warrant where there was probably cause that the computer contained evidence of a crime, where the agent merely copied the data before subsequently obtaining a search warrant, and where there was reason to believe that delay could lead to the destruction or loss of evidence).

[70] One of the companies whose computers he had hacked was located in Vernon, Connecticut.

[71] United States v. Ivanov, 175 F. Supp. 2d 367, 373 (D. Conn. 2001).

the challenges of preventing, investigating, and prosecuting cyber crime."[72] In order to prosecute computer crimes, it is necessary to preserve the integrity of the computer evidence, which may involve recovering documents in cache files, swap files, temporary files, unallocated space, or slack space.[73] 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 would be 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 a key tool for dealing with cross-border evidence requests. But MLATs are of limited efficacy in the cyber context[74]: MLAT requests are slow to process, are often limited to "dual incrimination" cases or cases that qualify as a crime in both the requesting and receiving countries, and are only useful when countries have explicit bilateral arrangements—a requirement at odds with the global nature of the Internet.[75] The United States, for instance, takes an average of ten months—and sometimes much longer—to comply with valid electronic

[72] Abraham D. Sofaer & Seymour E. Goodman, *Cyber Crime and Security: The Transnational Dimension*, *in* THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 1, 2 (2001); *see also id.* at 17 ("Even states with advanced economies, and heavily reliant on information technology, have failed to take steps necessary to protect themselves and others from attacks, thereby becoming weak links in the chain of security, or places where criminals and terrorists are able to attack other states with impunity.").
[73] R.E. Bell, *The Prosecution of Computer Crime*, 9 J. FIN. CRIME 308, 311 (2002).
[74] Susan Brenner has described MLATs as "so unsuitable as to be almost futile with regard to cybercrime and cybercriminals." Brenner, *supra* note 38, at 209.
[75] Bell, *supra* note 73, at 12-13.

evidence records requests from other countries pursuant to MLATs.[76] Such waiting times represent "an eternity in internet time"[77] and can not only delay investigations and prosecutions but also lead to the potential loss of fragile digital evidence.[78]

Second, foreign governments may thwart prosecutions under domestic criminal law by refusing to cooperate with investigations or to extradite the accused. Without cooperation from foreign governments in gathering and processing digital forensic evidence located abroad and in executing with warrants and subpoenas, it can be difficult to give effect to domestic laws. More problematic still is the extradition of foreign citizens. Russia's refusal to extradite its citizens has repeatedly proven an obstacle to U.S. prosecution of Russian hackers. Occasionally, extradition treaties with other countries have enabled the United States to arrest and prosecute Russian cyber criminals. For example, in 2009, American agents traveled to Russia to discuss their investigation of Roman Seleznev, a Russian hacker who stole millions of credit card numbers and sold them on an online black market. Though Russia refused to cooperate, the U.S. ultimately arrested Seleznev in the Maldives, which agreed to extradite him, and in August 2016, a Seattle jury

---

[76] *Liberty and Security in a Changing World*, REP. AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227 (Dec. 12, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

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

[78] *See* Brenner, *supra* note 38, at 211 ("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.").

convicted Seleznev of several counts.[79] Similarly, in July 2013, Russian hacker Aleksandr Andreevich Panin, who created and distributed the banking malware Trojan SpyEye, was arrested on vacation in the Dominican Republic and extradited to the United States. He pled guilty to conspiring to commit wire and bank fraud and was sentenced to over nine years in prison.[80]

Successful extraditions are rare, however. More commonly, as the following cases reveal, the United States issues arrest warrants or indicts cybercriminals in absentia, without the perpetrators ever facing jail time. In 2014, the F.B.I. issued an arrest warrant for Russian national Evgeniy Bogachev, charging him with distributing malicious software via phishing emails. The so-called "GameOver Zeus" malware stole personal information, including bank account login information. It is thought to have caused over $100 million in economic losses and, at its peak, to have infiltrated between half a million and a million computers.[81] Notwithstanding the U.S. government's offer of a $4.2 million bounty, Bogachev apparently continues to live in a seaside town on Russia's Black Sea coast and has not faced prosecution.[82]

---

[79] Christine Clarridge, *Son of Russian Parliament Member Convicted in Massive Hacking, ID-Theft Scene*, SEATTLE TIMES (Aug. 25, 2016 11:37AM), http://www.seattletimes.com/seattle-news/crime/seattle-jury-convicts-russian-man-of-massive-business-hacking-id-theft-scheme.

[80] Kate Brumback, *Creator of Malware Used to Drain Bank Accounts Gets 9 Years*, ASSOCIATED PRESS (Apr. 20, 2016 6:16 PM), http://bigstory.ap.org/article/542d00b1eac444ad85661ad9c18ba1f3/creator-malware-used-drain-bank-accounts-gets-9-years.

[81] Brian Krebs, *Inside the $100M 'Business Club' Crime Gang*, KREBS ON SECURITY (Aug. 15, 2015, 5:12PM), http://krebsonsecurity.com/2015/08/inside-the-100m-business-club-crime-gang.

[82] Alistair Stevenson, *The FBI Is Offering $4.2 Million for Info on the Creator of the World's Most Infamous Malware*, BUSINESS INSIDER (July 2, 2015, 9:39AM), http://www.businessinsider.com/fbi-zeus-cyber-crime-malware; Mansur Mirovalev & Colin Freeman, *Russian Hacker Wanted By US Hailed As Hero at Home*, Telegraph (June 7,

Last summer, Dmitry Ukrainsky, a Russian cybercriminal suspect, was arrested in Thailand, raising hopes among American prosecutors that they would be able to put him on trial in New York. Russian authorities, however, persuaded Thailand not to extradite him, maintaining that Ukrainsky should be prosecuted at home. In October 2016, Yevgeniy Aleksandrovich Nikulin, charged with hacking computer networks at three Internet companies, was arrested in the Czech Republic. The Czech Republic must now decide whether to extradite in accordance with the FBI's wishes or to return him to Russia.[83] Most recently, in March 2017, a California jury indicted four foreign nationals, including two officers of the Russian Federal Security Service, for hacking Yahoo's network and stealing information from approximately 500 million e-mail accounts.[84] The indictments mark the first U.S. criminal cyber charges against Russian government officials, but, since the officials remain in Russia, extradition is unlikely.

Russia is also not the only country protecting hackers with ties to the government. In May 2014, the United States indicted five Chinese military hackers on charges of economic espionage, in its first ever indictment of state actors for

---

2014, 7:00PM), http://www.telegraph.co.uk/news/worldnews/europe/russia/10883333/Russian-hacker-wanted-by-US-hailed-as-hero-at-home.html (quoting a policeman stating "I'd pin a medal on the guy").

[83] Jason Hovet & Petra Vodstrcilova, *U.S., Russia Request Czechs Extradite Arrested Russian Hacker*, REUTERS (Nov. 23, 2016, 5:43 PM), http://in.reuters.com/article/czech-usa-russia-cybercrime-idINKBN13I0VZ.

[84] U.S. Dep't of Just., *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts* (Mar. 15, 2017), http://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

cyber theft.[85] Robert E. Anderson, Jr., then a cybercrime investigator at the FBI, admitted that "[t]he chance of us ever getting those Chinese guys is about zero."[86]

As these examples illustrate, domestic criminal law is often an ineffectual tool when it comes to bringing foreign cyber criminals to justice in the United States. Even if legislative and adjudicative jurisdiction can be established, and a judgment is entered against the perpetrator, the prosecuting country may be unable to enforce that 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. . . . [F]or almost all users, there will be no threat of extraterritorial legal liability because of a lack of presence in the regulating jurisdictions. [87]

To sum up, domestic criminal law works when a perpetrator commits a crime in one jurisdiction, and that jurisdiction is empowered to investigate the crime and arrest the perpetrator. Transnational cyber aggressions, however, cross

---

[85] U.S. Dep't of Justice, U*.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (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").

[86] 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

[87] 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).

borders, giving rise to jurisdictional overlap and conflict. For these acts, "[t]he actions of individual states are insufficient"[88]: solutions lie beyond domestic criminal law.

III. Transnational Cyber Incidents: Three Case Studies

Part II demonstrated, from a theoretical perspective, that transnational cyber aggressions confound the application of the standard legal tools of domestic criminal law or the law of armed conflict. This Part uses three case studies—the Love Bug Attack, the DDoS attacks on Estonia, and the recent ransomware attack—to exemplify the problem of cyber attacks that cause significant global impact and yet get carried out with impunity. These cases thus point up the shortcomings of existing legal regimes and the need for new transnational and international solutions for criminalization and prosecution.

a. Love Bug Attack

In the absence of international cooperation, cyber criminals can engage in criminal activities with impunity. One of the most notorious examples of such impunity is the case of Onel de Guzman. As a student at the Amable Mendoza Aguiluz (AMA) Computer University in the Philippines, de Guzman wrote a program designed to steal Internet passwords that he submitted as his thesis and that got rejected. 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

[88] Sofaer & Goodman, *supra* note 72, at 30.

Windows computers, scanning computers for log-in names and passwords, destroying image and sound files, and then spreading via e-mail attachment to everyone in the user's address book. Internet Service Providers traced the virus to de Guzman, who admitted to releasing the virus.[89] While Philippine law enforcement initially pressed charges, the Philippine Department of Justice was ultimately forced to drop all charges because Philippine law at the time did not prohibit computer hacking. The Philippines quickly tried to correct its mistake; on June 14, 2000, Philippine President Joseph Estrada signed the Electronic Commerce Act, outlawing computer crimes, but because the Act did not apply retroactively, it could not cover de Guzman. Meanwhile, the U.S. Department of Justice charged de Guzman in absentia, but could not obtain an extradition treaty for Guzman since his actions were not illegal under the law of the Philippines.

The reach of ILOVEYOU was vast. The virus reportedly penetrated at least fourteen federal agencies in the United States, in addition to foreign governments like the British Parliament and 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.[90] All told, the virus may have cost as much as $10 billion

---

[89] 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)

[90] *The Love Bug Virus: Protecting lovesick Computers from Malicious Attack: Hearing Before the House Subcomm. on Technology of the Comm. on Science*, 106th Cong. 12 (2000) (statement of Keith A. Rhodes, Director, Office of Computer and Information Technology Assessment).

in damage.[91] Yet de Guzman escaped punishment. The story of de Guzman and the Love Bug virus thus typifies the problems of territorial jurisdiction. Territorial jurisdiction is in a sense overprotective, insofar as de Guzman subjected himself to the laws of every jurisdiction to which the virus may have spread. The fact that de Guzman was charged in absentia in the United States proves his vulnerability to prosecution in foreign jurisdictions. Actions that de Guzman took without leaving his home thus exposed him to multiple potential criminal prosecutions in countries with different—and perhaps conflicting—laws, with which de Guzman was likely unfamiliar. At the same time, territorial jurisdiction is underprotective. De Guzman evaded punishment altogether, because countries that were negatively impacted by the virus, like the United States, were unable to extradite him. When applied to transnational cyber aggressions, territorial jurisdiction leads, theoretically, to excessive possibilities for liability, even as it leads, practically, to impunity.

b. 2007 Attack on Estonia

In April 2007, a number of Estonian websites belonging to the Estonian parliament and government ministries as well as to newspapers, universities, and financial institutions, were subject to a series of cyber attacks. The attacks, which included DDoS attacks, continued in waves for three weeks and inflicted significant damage, demonstrating for perhaps the first time that cyber weapons represent a viable alternative to traditional weaponry. As Jeffrey Kelsey explained, "[t]his attack was more than just an inconvenience to the Estonian population: the emergency

[91] Kevin Poulsen, *May 4, 2000: Tainted 'Love' Infects Computers*, WIRED (May 3, 2010 8:00PM), http://www.wired.com/2010/05/0504i-love-you-virus/.

number, used to call for ambulances and the fire service, was unavailable for more than an hour."[92]

According to a spokeswoman for the Estonian Informatics Centre, which administers the country's information systems, the attack involved zombie computers in as many as 178 countries.[93] Estonia's foreign minister, Urmas Paet, accused Russians of orchestrating the cyber attacks, supposedly in retaliation for Estonia's decision to move the Bronze Soldier of Tallinn, a Russian World War II memorial, to the outskirts of the city. Estonia requested assistance from Russia in investigating the attacks, pursuant to a Mutual Legal Assistance Treaty between the two countries, but Russia refused assistance.

In March 2009, Sergei Markov, a Duma Deputy from the pro-Kremlin Unified Russia party, surprised the audience at an information warfare conference by pinning responsibility for the 2007 Estonian cyber attack on his assistant. "Don't worry, that attack was carried out by my assistant," Markov reportedly said, explaining that his assistant had decided that "something bad had to be done to these fascists."[94] A few days later, Markov confirmed to various news outlets that

---

[92] 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).
[93] Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FT (Mar. 11, 2009 2:00AM), http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?ft_site=falcon&desktop=true#axzz4a8YVDx00.
[94] Robert Coalson, *Behind the Estonia Cyber Attacks*, Radio Free Europe (Mar. 6, 2009), http://www.rferl.org/a/Behind_The_Estonia_Cyber attacks/1505613.html.

the perpetrators of the Estonia attack were Konstantin Goloskokov and other members of Russia's Nashi youth group.[95]

Like the Love Bug attack, the Estonia attacks reveal the shortcomings of existing responses to cyber hostilities. Goloskokov and his collaborators were never punished for their acts; indeed, Markov initially refrained from giving Goloskokov's name "because then he might not be able to get visas,"[96] suggesting that the only consequences Markov envisioned were travel restrictions. Nor could Estonia justifiably retaliate against Russia: while Estonia was apparently correct in blaming Russian nationals, it is less clear "whether the Russian government officially sanctioned the strike."[97] Transnational cyber aggressions like the Estonia attacks, carried out by individuals or non-state actors located outside the target country, underscore the limits of territorial jurisdiction and demand more creative solutions.

c. May 2017 Ransomware Attack

Just days ago, on Friday, May 12, 2017, a "ransomware" attack struck computers across much of Europe and Asia. So far, it has hit an estimated 200,000 computers in more than 150 countries.[98] Ransomware is computer malware that

---

[95] Chuck Miller, *Russia. Confirms Involvement with Estonia DDoS Attacks*, SC MEDIA (Mar. 12, 2009), http://www.scmagazine.com/russia-confirms-involvement-with-estonia-ddos-attacks/article/555577/.
[96] Coalson, *supra* note 94.
[97] Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War*, 9 GEO. J. INT'L AFF. 121, 123 (2008).
[98] David E. Sanger, Sewell Chan & Mark Scott, *Ransomware's Aftershocks Feared As U.S. Warns of Complexity*, N.Y. TIMES (May 14, 2017), https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html.

spreads covertly and holds victims' computer data hostage by locking their screen ("locker ransomware") or encrypting their files ("crypto ransomware"). This particular variant of ransomware, called Wanna Decryptor, is encryption-based malware that spreads via e-mail. Once inside the system, it creates encrypted copies of files that require a decryption key, deletes the original files, and leaves instructions demanding approximately $300 in Bitcoin as ransom to access the decyrytor. The malware has infected telecommunications and utility companies, banks, universities, government offices, electronic payment machines at gas stations and rail companies, and more. In England, Wanna Decryptor severely disrupted the National Health Service: doctors were unable to access patients' files, ambulances were delayed, and several hospitals were forced to turn people away at the emergency room. Russia was also hit especially hard: approximately 1,000 computers in Russia's Interior Ministry were targeted, in addition to computers at major Russian mobile phone and electronics retailers.

While the May 2017 Wanna Decryptor attack was especially serious, ransomware is becoming an increasingly common cyber threat. According to one estimate, as many as 40 percent of companies worldwide have been targeted by ransomware attacks.[99] Governments are also increasingly susceptible to ransomware attacks: state and local government networks are purportedly nearly

---

[99] Victoria Woollaston, *Wanna Decryptor: What is the Ransomware Behind the NHS Attack?*, WIRED (May 12, 2017), http://www.wired.co.uk/article/wanna-decryptor-ransomware.

twice as likely to be infected with malware or ransomware than small or medium-sized businesses.[100]

The Wanna Decryptor attack has cast a spotlight on transnational cyber aggressions. When an attack goes global in a matter of minutes, affecting individuals, businesses, and government entities in more than 150 countries, the problems of territorial jurisdiction, and the need for alternatives, are brought into stark relief.

IV. Accountability for Transnational Cyber Aggressions: International Dispute Resolution

As the previous Parts have shown, neither international humanitarian law nor domestic criminal law effectively regulates or deters transnational cyber aggressions. In the face of this challenge, some scholars have thrown up their hands, concluding that cyberspace is "a largely ungovernable space" and that prevention is the only option.[101] While prevention is of course essential, it must be coupled with some form of accountability, if we wish to avoid a Hobbesian world in which victims of cyber attacks take it upon themselves to hack back.[102] Put bluntly, unless there is a forum to which businesses can bring complaints, a promise of criminal sanctions,

---

[100] *Malware, Ransomware Twice As Likely to Hit State, Local Networks*, GCN (Dec. 1, 2015), http://gcn.com/articles/2015/12/01/sled-ransomware.aspx.
[101] MARINELLA MARMO & NERIDA CHAZAL, TRANSNATIONAL CRIME AND CRIMINAL JUSTICE 66 (2016).
[102] *See* THOMAS HOBBES, THE LEVIATHAN (1651) (describing the state of nature as a war of all against all).

or some other pressure valve to release victims' frustration, victims of cyber attacks will increasingly resort to cyber-vigilantism.[103]

This Part sketches possible solutions to the problem of regulating transnational cyber aggressions. 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 aggressions 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 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

[103] 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 77, at 140. Conversations at the Yale Cyber Leadership Forum just weeks ago 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).

arbitration regime was established under the aegis of intergovernmental organizations like the United Nations and the Permanent Court of Arbitration, countries used civil arbitration to regulate transnational activity and resolve disputes. Indeed, the practice of international arbitration extends back to antiquity, when disputing Greek city-states would call upon the federal government (the Achaean Council) or an independent state to arbitrate territorial disputes.[104] International arbitration was brought back with the 1794 Jay Treaty between Britain and the United States, which established international arbitral commissions to resolve boundary disputes and disputes over wartime debts.[105]

International arbitration is not only for disputes between nations, however; international civil arbitration can also be used to hold private actors accountable. In the early nineteenth century, Britain entered into a number of bilateral treaties to establish international slave trade commissions. Under these treaties, 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.[106] If the

---

[104] *See* N.G.L. Hammond, *Arbitration in Ancient Greece*, 1 ARBITRATION INTERNATIONAL 188, 188-89 (1985).

[105] Treaty of Amity, Commerce, and Navigation, U.S.-Gr. Brit., Nov. 19, 1794, 8 Stat. 116.

[106] *See* Eugene Kontorovich, *The Constitutionality of International Courts: The Forgotten Precedent of Slave-Trade Tribunals*, 158 U. PA. L. REV. 39 (2009). The United States initially refused to join this regime. President John Quincy Adams believed the mixed courts would be unconstitutional because they did not provide for appeal to Article III courts or for the procedural protections of the Bill of Rights. *Id*. at 77-80. Eventually, however, the United States agreed to join the regime and, in 1862, President Lincoln signed the Lyons-Seward Treaty with Great Britain. Justifying the changed attitude toward the constitutionality of such a treaty, Senator Charles Sumner explained that "the question was less understood" in the 1820s and that the Supreme Court has since then affirmed the constitutionality of territorial courts, undercutting arguments about the exclusivity of Article III. 6 THE WORKS OF CHARLES SUMNER 482 (1872); *see, e.g.*, Am. Ins. Co. v. 356 Bales of Cotton, 26 U.S. 511, 546

seizure was unlawful, the "Seizor" was liable for payments. As these historical example suggest, international arbitral commissions can play an important role in adjudicating international disputes and punishing wrongdoers, without impermissibly undermining state sovereignty.

Today, international arbitration under the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958,[107] more commonly known as the New York Convention, offers perhaps the most successful modern form of international dispute resolution.[108] As of April 2017, 157 nations have ratified the Convention.[109] Enacted to promote international uniformity in the treatment of arbitral awards, the New York Convention imposes two sets of rules on national courts of States parties. First, national courts in member States must recognize arbitration agreements made between the parties. When confronted with a dispute governed by the arbitration agreement, courts must refer the parties to arbitration if either party so requests.[110] Second, under Article III, the Convention requires States parties to recognize and enforce arbitral awards issued in the territory of another State.[111] The Convention thus enables prevailing parties to collect on the assets of the losing party, even where the latter resides in another

(1828) (upholding the constitutionality of a territorial court whose judges lacked life tenure).

[107] June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38

[108] Michael John Mustill, *Arbitration: History and Background*, 6 J. INT'L ARB. 43, 49 (1989) (describing the New York Convention as described as "the most effective instance of international legislation in the entire history of commercial law").

[109] *Convention on the Recognition and Enforcement of Foreign Arbitral Awards,* UNITED NATIONS TREATY COLLECTION, http://www.newyorkconvention.org/countries [hereinafter New York Convention].

[110] New York Convention, art. 2(3).

[111] New York Convention, art. 3.

jurisdiction. Even as the Convention mobilizes national courts to effectuate arbitral awards, it limits the scope of national judicial supervision by limiting the evidence and the substantive defenses that national courts can consider in enforcement proceedings.[112]

The New York Convention offers a well-functioning, widely adopted system of civil accountability for transnational wrongs that could be harnessed to promote accountability for transnational cyber aggressions. 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, 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.

---

[112] Michael Reisman, *Preface*, *in* ENFORCEMENT OF ARBITRATION AGREEMENTS AND INTERNATIONAL ARBITRAL AWARDS: THE NEW YORK CONVENTION IN PRACTICE (Emmanuel Gaillard & Domenico di Pietro eds., 2008), 1, 1.

Significantly, there is precedent for tying a specialized arbitral scheme to the New York Convention: the Court of Arbitration for Sport (CAS) harnesses the machinery of the New York Convention to punish violators of international athletic norms.[113] Founded in 1984 by Judge Kéba Mbaye of the International Court of Justice and then-President of the International Olympic Committee, Juan Antonio Samaranch, CAS is an impartial, independent body dedicated to resolving international sports-related disputes quickly and cost-effectively.[114] It is widely regarded as the final decision-maker for international sports-related disputes, to the exclusion of national courts.[115] As with any arbitral proceeding, the parties must consent to have their dispute heard by the CAS.[116] Once the CAS renders a judgment, sports organizations can enforce the judgment directly—for example, through registration or playing bans[117]—or parties can apply to national courts, typically the Swiss Federal Tribunal, for enforcement under the New York Convention.

We might imagine a specialized arbitral tribunal for cyber-related disputes, analogous to the CAS. A cyber arbitration body could issue civil penalties for cyber

---

[113] *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, 77.

[114] *See* Reilly, *supra* note 113, at 63.

[115] *See id.* at 67; Tribunal fédéral [TF] [Swiss Federal Tribunal] May. 27, 2003, III Arrêts du Tribunal Fédéral Suisse [ATF] 129 445 (Switz.), translated into English in MATTHIEU REEB, DIGEST OF CAS AWARDS III, 2001-2003 688 545 (2004) (dismissing a challenge by two Russian athletes to a Court of Arbitration for Sport award and asserting that CAS was to be regarded as a real arbitral court, whose awards are comparable to state court judgments).

[116] 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 113, at 66-67.

[117] *Id.* at 76 & n.66.

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 could benefit from arbitrators with technology expertise. Over time, a jurisprudence of the cyber tribunal could develop, contributing to the elaboration of this specialized body of law, as with the publication of CAS appellate decisions.[118]

A cyber arbitration scheme could also be tailored to the unique features of transnational cyber aggressions. Individuals, corporations, or states could all bring suit against perpetrators. Class actions could also be permitted, allowing parties affected by a cyber attack to aggregate their claims to meet harm thresholds and, conceivably, to financially wipe out cyber villains. We could even conceivably imagine 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. In this sense, a civil arbitration system could reach more broadly than a criminal liability regime that would require criminal intent.

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 is a specialized agency that promotes international cooperation relating to telecommunications infrastructure and global technical standards. It currently has members from 193 countries and approximately 700

[118] Awards issued under the Ordinary Arbitration Procedure are not generally made publicly available.

public and private entities. The ITU has used its technical expertise to support less technically sophisticated countries and to engage in Internet-related research and development. For example, the ITU in 2014 announced the creation of a Global Cybersecurity Index (GCI) to evaluate and compare cybersecurity strategies worldwide. Additional ITU activities include capacity building and helping countries establish national Computer Incident Response Teams (CIRTs). Based on initiatives like these, there has been talk in recent years of the International Telecommunications Union taking on a bigger role in Internet regulation.

Proposals for the ITU to regulate the Internet have prompted outcries from those concerned that such regulation would destroy the open, decentralized governance system that the Internet has relied on since the days of NSFNET.[119] 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 "correct historical imbalances" relating to the "dominance of the U.S." over the Internet.[120] If international resistance could be overcome, however, the ITU would seem to be a natural entity to call upon to develop cyber regulations and arbitrate disputes.

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

---

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

[120] Sheetal Kumar, *Cybersecurity: What's the ITU Got to Do With It?* (July 9, 2015), https://www.gp-digital.org/cybersecurity-whats-the-itu-got-to-do-with-it/.

resolution. The Internet Engineering Task Force (IETF), 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 system to resolve disputes relating to trademarks and the registration of Internet domain names. The UDRP administrative adjudication process could serve as a model for arbitrating disputes involving transnational cyber aggressions. As of October 1, 2016, ICANN is no longer subject to U.S. government oversight,[121] potentially making it potentially 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 arbitration system for transnational cyber aggressions could transfer the costs of wrongful conduct from victims to perpetrators. By permitting injured parties to seek redress for losses, an international civil liability scheme would obviate the temptation to hack back, while the potential for individual victims to aggregate claims and obtain significant damages awards could meaningfully deter would-be cyber attackers. An international arbitration system, potentially tied to the New York Convention and modeled after the Court of Arbitration for Sport, could

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

thus offer one tool in the legal arsenal for responding to transnational cyber aggressions.

b. Transnational Criminal Law

In addition to civil remedies for victims, a robust liability scheme for transnational cyber aggressions also includes criminal law penalties. As Parts II and III showed, reliance on individual states applying 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.[122] 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.[123]

Transnational criminal law can be understood through the lens of transnational legal theory. Non-state actors, including intergovernmental organizations, non-governmental organizations, and non-profits, can serve as

[122] Brenner, *supra* note 38, at 209.
[123] *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").

transnational norm entrepreneurs,[124] shaping international norm development and promoting compliance with international law through the development of national law. As "agents of internalization," transnational norm entrepreneurs have an important role to play in formulating policy, monitoring compliance, and pushing countries to move toward "habitual internalized compliance with international rules."[125] The role of transnational norm entrepreneurs may be particularly important where the policy areas are technically complex and present significant noncompliance incentives,[126] as with Internet regulations.

Legal harmonization is an important part of developing a transnational criminal law of cyber. 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, particularly in the cyber context, given the likelihood of an offense taking place outside the jurisdiction where the accused is located. 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

---

[124] *See, e.g.*, Harold Hongju Koh, *Bringing International Law Home*, 35 HOUS. L. REV. 623, 648 (1998) (focusing on the role of transnational norm entrepreneurship in internalizing international norms in domestic settings); Melissa A. Waters, *Mediating Norms and Identity: The Role of Transnational Judicial Dialogue in Creating and Enforcing International Law*, 93 GEO. L.J. 487, 499-505 (2005) (emphasizing the role that transnational norm entrepreneurs can play in exporting domestic norms and thereby shaping international norm development).

[125] Harold Hongju Koh, *Opening Remarks: Transnational Legal Process Illuminated*, *in* TRANSNATIONAL LEGAL PROCESSES 327-28 (Michael Likosky ed., 2002); *see also* .

[126] Jonas Tallberg et al., *Explaining the Transnational Design of International Organizations*, 68 INT'L ORG. 741, 754 (2014).

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 assimilating those norms into domestic law are examples of 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 aggressions.

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 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.[127] The 24/7 network is just a first step: the United Nations General Assembly has repeatedly called for a global

[127] Thomas Dougherty, U.S. Dep't of Justice, *G8 24/7 Cybercrime Network*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680303ce2; *see also* U.S. Dep't of Justice, *Attorney General Loretta E. Lynch Delivers Remarks at Leiden University Student Forum* (June 1, 2016) https://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-leiden-university-student-forum (describing the 6-8 cyber network as a "rapid reaction system" that has grown to include over 70 countries). In the first two months of 2014, the United States received over 100 requests and issued over 25 requests to other countries. Dougherty, *supra*.

framework to protect cyber infrastructure and combat cybercrime.[128] In 2000, a group of experts gathered at Stanford University to draft a "Proposal for an International Convention on Cyber Crime and Terrorism."[129] Among the Stanford team's proposals was the establishment of an international agency to protect information infrastructure and to develop standards concerning cyber security.[130] Several countries have also formed interjurisdictional task forces to address transnational cybercrime,[131] and the International Telecommunication Union has drafted model cybercrime legislation and compiled resources to assist countries in drafting their own cybercrime laws and procedural rules.[132]

The most important step toward a transnational criminal law of cyber to date is the Budapest Convention on Cybercrime.[133] Drafted by the Council of Europe and

---

[128] *See, e.g.*, "Combating the criminal misuse of information technologies," United Nations, General Assembly Resolution 56/121, A/RES/56/121 (Jan. 23, 2002), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf; "Combating the criminal misuse of information technologies," United Nations, General Assembly Resolution 55/63, A/RES/53/63 (Jan. 22, 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf; "Creation of a global culture of cybersecurity," United Nations, General Assembly Resolution 57/239, A/RES/57/239 (Jan. 31, 2003), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf; "Creation of a global culture of cybersecurity and the protection of critical information infrastructures," United Nations, General Assembly Resolution 58/199, A/RES/58/199 (Jan. 30, 2004), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

[129] Abraham D. Sofaer, Seymour E. Goodman et al., *A Proposal for an International Convention on Cyber Crime and Terrorism*, Hoover Institution, Stanford University (Aug. 2000), http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf.

[130] *Id*. at art. 12.

[131] 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/.

[132] *See* International Telecommunication Union, *ITU Toolkit for Cybercrime Legislation* (2010).

[133] Convention on Cybercrime, Council of Europe, ETS No. 185 (Nov. 23, 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [hereinafter Budapest Convention].

adopted in 2001, the Budapest Convention has so far been ratified or acceded to by 54 states, largely, but not exclusively, in Europe.[134] The United States was one of the original signatories in November 2001 and eventually ratified the convention in 2006.

The Budapest Convention represents, in Secretary of State John Kerry's words, "the best . . . legal framework for working across borders to define what cyber crime is and how breaches of the law should be prevented and prosecuted."[135] The Convention assumes that criminal prosecutions will continue to take place at the level of the nation-state, but aims to harmonize national laws and promote international cooperation on evidence-gathering. Article 22, paragraph 1 gives member states jurisdiction over any offense that has occurred in their territory, regardless of where the attacker may be 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.[136] Further, the Convention facilitates mutual assistance and extradition by allowing for the

[134] Council of Europe, *Chart of Signatures and Ratifications of Treaty 185—Convention on Cybercrime* (Apr. 20, 2017), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
[135] *An Open and Secure Internet: We Must Have Both*, Remarks by John Kerry, Secretary of State, at Korea University, Seoul, South Korea (May 18, 2015), http://www.state.gov/secretary/remarks/2015/05/242553.htm.
[136] Budapest Convention, art. 22(1).

Convention itself to be used as an extradition or legal assistance treaty in the absence of any preexisting MLAT between the relevant states.[137]

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.[138] Until the Convention on Cybercrime is universally adopted, countries like Russia and China can continue to shelter cyber criminals from prosecution.[139] Additionally, even 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.[140] Lastly, the Convention provides only vague definitions of several key terms, and does not detail the elements required for various offenses, leaving it

[137] Budapest Convention, arts. 24(3), 27(1).
[138] *See Russia Prepares New UN Anti-Cybercrime Convention – Report*, RT (Apr. 14, 2017), https://www.rt.com/politics/384728-russia-has-prepared-new-international. The Russian Foreign Ministry prepared its own draft convention, which it presented to UN experts in April 2017. The Russian draft convention proposes various forms of international cooperation such as information-sharing about criminal activities and lists s, including the creation of viruses and malware and disruption to the work of computer networks, but it also 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*.
[139] *See* SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 210 (2010).
[140] 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).

to individual states' discretion.[141] 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.[142] 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,[143] while Article 32 allows law enforcement in one member state to conduct an extraterritorial investigation in another state without notifying that state's authorities.[144] 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.[145] Many other commentators and civil liberties groups, however, have raised privacy concerns, objecting to the fact

---

[141] *See, e.g.*, Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 J. High Tech. L. 101, 113 (2003).
[142] Marion, *supra* note 140, at 704.
[143] Budapest Convention, art. 21(1).
[144] Budapest Convention, 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.").
[145] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 166 (2006).

that the Convention incorporates the United States' lesser privacy protections rather than Europe's higher standards of data protection.[146]

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.[147] The Convention also does not prevent member states from submitting to stricter privacy standards, as can be found in the Council of Europe's Data Protection Convention.[148]

Moreover, from a U.S. perspective at least, international cooperation could potentially promote rather than undermine respect for individual privacy. Perpetrators of transnational cyber aggressions 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 is not protected under the Fourth

---

[146] *See, e.g.*, Marion, *supra* note 140, at 705; Brenner, *supra* note 74, 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).
[147] Budapest Convention, art. 15.
[148] 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.

Amendment,[149] nor are communications that have been received by the intended recipient.[150] 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 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.[151] 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 from other countries when relevant to an ongoing investigation, it may be more likely to try to obtain more data across the board, and to retain that data for indefinite periods.[152] Thus, rather than enabling law enforcement to evade Fourth Amendment privacy protections for U.S. residents by relying on other countries, international

---

[149] *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.").

[150] *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").

[151] Law enforcement can also obtain consent to electronic searches from infrastructure providers that own relevant 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).

[152] *Cf.* United States v. Ganias, 755 F.2d 125 (2d Cir. 2014) (holding that the Fourth Amendment does not permit officials searching and seizing an electronic device to "indefinitely retain every file on that computer for use in future criminal investigations").

cooperation on cyber investigations could in fact enable 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 one's computer and access files with impunity, allowing law enforcement to collect, review, and share data subject to strict procedural rules may be preferable.

To sum up, 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, like requiring countries to assist with national 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 aggressions. But 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 an important instrument for fighting cybercrime.

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, or before a *sui generis* international criminal tribunal for cyber.

The development of international criminal tribunals is a fairly recent phenomenon. As early as 1948, the United Nations General Assembly recognized the need for an international criminal court, and charged the International Law Commission with "study[ing] the desirability and possibility of establishing an international judicial organ for the trial of persons charged with genocide . . . ."[153] The idea languished for several decades, however, and it was not until 1998, following the conflicts in Rwanda and the former Yugoslavia, that the General Assembly met in Rome to draft a statute for a new international criminal tribunal. The Rome Statute establishes the jurisdiction of the International Criminal Court (ICC) over four crimes—the crime of genocide, crimes against humanity, war crimes, and crimes of aggression.

Presently, the ICC would probably not have subject-matter jurisdiction over cyber crimes. Cyber aggressions are not specifically recognized anywhere in the Rome Statute and likely do not fit any of the categories of crimes the ICC can hear. As originally drafted, the Rome Statute listed the crime of aggression in Article 5 as

[153] G.A. Res. 260 (Dec. 9, 1948).

one of the four crimes over which the ICC had jurisdiction, but did not provide a definition of the crime that would enable prosecutions. After the Rome Statute entered into force in 2002, the States parties established a Special Working Group on the Crime of Aggression (SWGCA) to draft a definition of the crime and set out the conditions under which the ICC would exercise jurisdiction. At a conference in Kampala in 2010, the States parties adopted a definition and jurisdictional regime for the crime of aggression. Since then, 33 States have ratified or accepted the amendments. The States parties must additionally activate the Court's jurisdiction by a two-thirds majority.

Assuming the Court'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."[154] By limiting potential culpability to those with direct political or military control, the so-called "leadership clause" excludes most perpetrators of cyber attacks. Cyber attacks rarely occur in the context of a strict chain of command: most are carried out "by individuals with only tenuous affiliations to a collective,"[155] 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

[154] *See* Rome Statute, art. 8 bis (1) (entered into force July 1, 2002), rev. 2010.
[155] Ophardt, *supra* note 32, at 16-17.

people.[156] Still, in most cases, limiting ICC jurisdiction to high-level state actors prevents regulation even of cyber attacks with major international repercussions.

An additional problem with relying on the crime of aggression is the list of actions provided in the Article 8 *bis* definition that qualify as acts of aggression. Those actions include an armed invasion, bombardment, and blockade by the traditional armed forces of another State. While the phrasing of the definition suggests that the list is exemplary not 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 cybercrime would not generally be. Cyber attacks resulting in physical damage could conceivably count as crimes against aggression if the list is 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, which defines war crimes, includes 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,[157] and attacks on civilian objects that are not military objectives.[158] To the extent a cyber attack destroys, rather than simply interfering with, civilian data and communications, cyber attacks carried out in the context of armed conflict could conceivably rise to the level of war crimes. But Article 22

[156] *Id.* at 18.
[157] Rome Statute, art. 8(2)(a)(iv).
[158] Rome Statute, art. 8(2)(b)(ii).

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.[159] As a result of this inflexibility, cybercrimes that were not explicitly contemplated in Article 8 would be unlikely to qualify as war crimes.[160] 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 aggressions.

The Rome Statute could be amended, however, to expand the jurisdiction of the International Criminal Court to cover grave cyber offenses. Another solution would be to create a new international criminal law tribunal with specialized competency in computer technology.[161] 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 Treaty on an International Criminal Court or Tribunal for Cyberspace.[162]

Whichever solution were adopted, the availability of an international criminal tribunal would mitigate many of the problems of nation-state jurisdiction,

---

[159] Rome Statute, art. 22.

[160] *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).

[161] *See, e.g.*, Stahl, *supra* note 9, at 272 (2011) ("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.").

[162] 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.

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.[163] Moreover, ICC investigations can expose government corruption and unwillingness to comply with international standards, eventually increasing domestic prosecutions in the intermediate term.[164] Thus, international criminal prosecutions of cyber criminals could help to deter acts of cyber aggression.

There are two ways in which an international criminal tribunal could obtain jurisdiction over alleged an alleged perpetrator of transnational cyber aggressions: universal jurisdiction and complementarity.

i. Universal Jurisdiction

Universal jurisdiction, recognized for centuries for piracy offenses, offers one solution to the problems of territorial jurisdiction when it comes to criminal liability.[165] Rooted in "the accused's attack upon the international order as a

---

[163] *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* (Working Paper 2015), https://commons.lib.niu.edu/bitstream/handle/10843/16390/INTL%20301%20%26%20401%20-%20ICC%20Capstone%20Paper.pdf.

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

[165] *See* Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 H. INT'L L.J. 183, 184 (2004); *compare* RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW (1965) (listing piracy as the only universal crime) *with* RESTATEMENT (THIRD)

whole,"[166] universal jurisdiction enables an international criminal tribunal (or the courts of any nation) to claim criminal jurisdiction over an accused, regardless of where the act 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[167]—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 well as under customary international law.[168] Cyber criminals, too, might be considered *hostis humani generis*: cyber space can be thought of as the modern-day "high seas," and transnational cyber aggressions the equivalent of pirates' indiscriminate acts of depredation.[169]

Scholars often assume that universal jurisdiction for piracy is only justified because no state has jurisdiction over the high seas.[170] However, the D.C. Circuit

---

OF FOREIGN RELATIONS LAW (1987) (enumerating several universal crimes, including war crimes and apartheid).

[166] ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 58 (1995).

[167] See EDWARD COKE, 3 INSTITUTES ON THE LAWS OF ENGLAND 113 (1797).

[168] United Nations Convention on the Law of the Sea, U.N. Doc. A/CONF. 62/122 (Dec. 10, 1982), art. 105. 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 (1987).

[169] *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).

[170] *See, e.g.*, Eugene Kontorovich, *An Empirical Examination of Universal Jurisdiction for Piracy*, 98 CAL. L. REV. 243, 253 (2010) (stating that "the international law of piracy applies only on the 'high seas'").

Court recently ruled that, since Article § 101(c) of UNCLOS, which criminalizes the facilitation of privacy, does not explicitly mention the high seas, aiding and abetting piracy does need not take place on the high seas to be illegal under the Convention.[171] 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 aggressions.

Perhaps a better justification for universal jurisdiction over piracy is that it endangers international trade.[172] Transnational cyber aggressions similarly threaten international trade, for example, when DDoS attacks disable access to major commercial websites or ransomware attacks threaten the destruction of international corporations' records and files. By the same logic, then, severely disruptive transnational cyber aggressions could properly be subject to universal jurisdiction.[173]

The challenge in applying universal jurisdiction to the cyber context, however, becomes defining the scope of threats for which universal jurisdiction is authorized narrowly enough to prevent countries like Russia and China from taking

[171] United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013)
[172] *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).
[173] *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.").

advantage of universal jurisdiction to shut down online dissent. If the crimes subject to universal jurisdiction could be carefully drawn, an international criminal tribunal that could hear those universal jurisdiction crimes and prosecute cyber criminals anywhere in the world under a consistent body of laws could prove a powerful deterrence mechanism.

ii. Complementarity

A second way of establishing jurisdiction over international crimes is complementarity, upon which the International Criminal Court 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.[174] As a result, complementarity is respectful of state sovereignty, and may make states more likely to join a protocol like the Rome Statute since they can retain control over matters of importance to them. Complementarity may also incentivize countries to adopt and enforce legislation—in this case, criminalizing transnational cyber aggressions—in order to keep cases in their own courts.

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

[174] Rome Statute of the International Criminal Court, Preamble para. 10, arts. 1, 15, 17, 18, & 19, July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

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 international court 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. 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 was committed by a national or on the territory of that state.[175] Precisely what it would mean for a cybercrime to be committed on a state's territory is not clear. If one formed a very broad conception of ICC jurisdiction, according to which the physical routing of attacks determines whether a state party to the Rome Statute was the site of a crime,[176] both the primary state victim and the state whose infrastructure was exploited could provide the jurisdictional hook. Since transnational cyber aggressions are often routed through a large number of

[175] Rome Statute, 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.
[176] *See* Ophardt, *supra* note 32, at 26.

territories,[177] the jurisdictional bar could often be overcome. But a crime with a merely incidental relationship to a country may not qualify as a crime committed in that state. Finally, even if it could properly exercise jurisdiction over a defendant who was not a national of a member state, the ICC could face the same extradition problems described in Parts II and III.

There are clearly significant challenges to prosecuting cyber criminals under international criminal law. International criminal tribunals are still new, however, and a new tribunal could potentially be created to hear cases of cyberterrorism[178] and other serious cybercrimes that threaten governmental institutions, cause large economic losses, or interfere with civilian Internet usage in significant ways. Were such a tribunal to exist, it would send a powerful message to the online community and could go a long way to ending impunity.

Conclusion

In the absence of a viable model for holding 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

[177] *Id.* at 22.
[178] *See* Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1 (2010).

may encounter conventional crimes properly subject to domestic criminal law as well as violations of the international law of armed conflict. Critically, however, the cyber context also presents a third category of wrongs that do not fit comfortably within either domestic criminal law or the law of armed conflict: transnational cyber aggressions.

The jurisdictional rules developed for the nineteenth century world of Westphalian nation-states are in many ways at odds with the inherently cross-border character of transnational cyber aggressions. Regulation and deterrence of transnational cyber aggressions requires novel legal solutions. While the elaboration and implementation of those solutions may seem like a formidable challenge, there is reason to be cautiously optimistic. Unlike many acts that the international community has sought to condemn, which harm countries disproportionately,[179] *no* country is immune from the threat of transnational cyber aggressions. The recent ransomware attack made clear that even supposed cybercrime havens may find themselves victim of transnational cyber aggressions. Thus, as the number of computer devices grows and the risks multiply, countries may face both internal and external pressures to develop and enforce a comprehensive international accountability regime.

[179] Climate change, for example, disproportionately harms small island nations, while the costs of restrictions on pollution and carbon emissions would be borne heavily by developing economies.