2013

Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm

Jan E. Messerschmidt

Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm

Shearman & Sterling Student Writing Prize in Comparative and International Law, Outstanding Note Award

Cyberespionage has received even greater attention in the wake of reports of persistent and brazen cyberexploitation of U.S. and Canadian firms by the Chinese military. But the recent disclosures about NSA surveillance programs have made clear that a national program of cyberdefense of private firms' intellectual property is politically infeasible. Following the lead of companies like Google, private corporations may increasingly resort to the use of self-defense, hacking back against cross-border incursions on the Internet. Most scholarship, however, has surprisingly viewed such actions as outside the ambit of international law. This Note provides a novel account of how international law should govern cross-border hacks by private actors, and especially hackbacks. It proposes that significant harm to a state's intellectual property should be viewed as "transboundary cyberharm" and can be analyzed under traditional international legal principles, including the due diligence obligation to prevent significant harm to another state's territorial sovereignty. Viewing cyber espionage within this framework, international law may presently permit states to allow private actors to resort to self-defense as proportionate countermeasures. By doing so, this Note offers a prescription for how states might regulate private actors to prevent unnecessary harm or

vigilantism while preserving the right of self-defense.

INTRODUCTION

We now know it as Unit 61398[1]—the premier cyber espionage entity within the Chinese People's Liberation Army.[2] In a gray, nondescript office tower in the Pudong district outlying Shanghai, some of the most sophisticated Chinese hackers, popularly known as "Comment Crew,"[3] have systematically stolen hundreds of terabytes of intellectual property from at least 141 companies in the United States and Canada.[4]

They are not alone. On January 12, 2010, Google, Inc. publicly announced that another group, now identified as the Elderwood Gang,[5] had infiltrated the company's network along with at least thirty other U.S. companies.[6] The attack, nicknamed "Operation Aurora,"[7] was traced to servers at two Chinese educational institutions.[8] But Google didn't stop at tracing the source of the attack. Launching a "secret counteroffensive," the company gained access to the source of the attack and obtained evidence that suggested possible Chinese

---

1. Formally, the unit was known as the 2nd Bureau of the People's Liberation Army's General Staff Department's 3rd Department. *See* David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2013, at A1.

2. *See* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, Feb. 18, 2013, 7–19 [hereinafter MANDIANT REPORT].

3. *See* Mark Clayton, *Stealing U.S. Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China*, CHRISTIAN SCI. MONITOR (Sept. 14, 2012), http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China. Hacking crews are commonly known by a variety of nicknames. Comment Crew is often referred to as Comment Group, and activities attributed to the group nicknamed "Shady Rat," may also be tied to Comment Crew. *See* MANDIANT REPORT, *supra* note 2, at 26.

4. MANDIANT REPORT, *supra* note 2, at 3, 9; *see also* Sanger, Barboza & Perlroth, *supra* note 1.

5. Elderwood Gang is also known as the Beijing Group and Sneaky Panda. *See* Clayton, *supra* note 3.

6. Riva Richmond, *Flawed Security Exposes Vital Software to Hackers*, N.Y. TIMES BITS BLOG (Mar. 5, 2010, 7:04 PM), http://bits.blogs.nytimes.com/2010/03/05/flawed-security-exposes-vital-software-to-hackers/.

7. George Kurtz, *Operation "Aurora" Hit Google, Others*, MCAFEE BLOG CENTRAL (Jan. 14, 2010, 3:34 PM), *available at* http://wirelessinnovator.com/index.php.

8. Tim Maurer, *Breaking Bad*, FOREIGN POLICY (Sept. 10, 2012), http://www.foreignpolicy.com/articles/2012/09/10/breaking_bad (last visited Jan. 16, 2012).

government involvement.[9] Matt Buchanan of the tech blog Gizmodo crowed, "it's pretty awesome: If you hack Google, they will hack your ass right back."[10]

Google's disclosure that it had hack*backed* raised eyebrows, to be sure, but the company does not appear to be alone. Private companies, including those listed on the Fortune 500, have increasingly turned to self-help measures in response to cyber intrusions.[11] A survey by CounterTack of information security executives found nearly a third of companies surveyed would be "well-served" if they could strike back,[12] and at a 2012 Black Hat conference in Las Vegas, a poll of 181 participants found that more than a third had engaged in hackbacks previously,[13] with some speculating that the numbers could be even higher.[14]

Hacking, and hacking *back*, raises a host of international legal questions,[15] but most scholarly attention has focused on whether

---

9. *See* David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 15, 2010), http://www.nytimes.com/2010/01/15/world/asia/15diplo.html; Ellen Nakashima, *U.S. Plans to Issue Official Protest to China Over Attack on Google*, WASH. POST, Jan. 16, 2010, at A4.

10. Matt Buchanan, *Google Hacked the Chinese Hackers Right Back*, GIZMODO (Jan. 15, 2010, 10:32 AM), http://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back.

11. *See Firewalls and Firefights*, ECONOMIST (Aug. 10, 2013), http://www.economist.com/news/business/21583251-new-breed-internet-security-firms-are-encouraging-companies-fight-back-against-computer [hereinafter ECONOMIST, *Firewalls and Firefights*]; Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law & Legal Theory Papers Series, Research Papers Series No. 08–20, 2009), *available at* papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932; *see also* Joseph Menn, *Hacked Companies Fight Back with Controversial Steps*, REUTERS, June 17, 2012; James Temple, *Hackers Getting Hacked by Security Firms*, S.F. CHRON. (Nov. 30, 2011), http://www.sfgate.com/business/article/Hackers-getting-hacked-by-secu rity-firms-2306472.php.

12. John Worrall, *New CounterTack Study: A Cyber-readiness Reality Check*, COUNTERTACK BLOG (Aug. 13, 2012, 8:02 AM), http://www.countertack.com/blog/bid/203331/New-CounterTack-Study-A-Cyber-readiness-Reality-Check.

13. Brian Prince, *Black Hat: Hacking Back—The Best Defense May Not be the Best Offense*, SECURITY WEEK (July 27, 2012), http://www.securityweek.com/black-hat-hacking-back-best-defense-may-not-be-best-offense.

14. *Id.* (quoting nCircle CTO Tim Keanini that because companies may not "want to admit they use retaliatory tactics," the number of companies pursuing these options could be even higher).

15. It also raises considerable domestic legal questions. *See generally* Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201 (2006). Hackbacks almost assuredly implicate possible violations of the Computer Fraud

states may counter-strike under the laws of armed conflict,[16] or as countermeasures under general international law.[17] Scholarship has been largely state-centric in this regard,[18] with surprisingly little writ-

---

and Abuse Act (CFAA), 18 U.S.C. § 1030 (prohibiting the unauthorized access of any "protected computer" where protected computer is defined as any computer used in or affecting interstate or foreign commerce), as well as the federal wiretap statute. That said, the CFAA's $5,000 damage threshold may preclude liability under the CFAA for many hackbacks, especially those that don't cause any direct damage or harm. *See* § 1030(a)(4). For a lively debate on the implications of hackbacks for the CFAA, see Stewart Baker, Orin Kerr & Eugene Volokh, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/. Significant cross-border hackbacks by states or non-state actors might also implicate neutrality laws. *See* 18 U.S.C. § 960; *see also infra* note 230 and accompanying text (discussing neutrality doctrine in relation to private hackbacks).

16. *See, e.g.*, Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1 (2009); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L. 207 (2002); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 487 (2012).

17. *See generally* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11 (2011); *see also* Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012).

18. *See, e.g.*, Michael N. Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SEC. L. 245–60 (2012); Hathaway et al., *supra* note 17; Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283–93 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012); Michael N. Schmitt, *The 'Use of Force' in Cyberspace: A Reply to Dr. Ziolkowski*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 311–17 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 443 (2011); Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569 (2011); Michael N. Schmitt, *Cyber Operations in the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89–110 (Raul Pedrozo & Daria Wollschlaeger eds., 2011); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues that Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 197 (2010); Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151–78 (2010); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87 (2010); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007); 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, 190 (2006); Vida M. Antolin-Jenkins, *Defining the Parameters of*

ten on the international legal dimensions of cyber conflict among non-state actors, especially when that hacking does not cause physical damage.[19]

This Note seeks to fill that gap, arguing that international law does, in fact, regulate both hacking and hacking back by private actors. To make this case, this Note makes two significant analytical moves. First, this Note argues that cross-border hacking, when causing harm to another state's intellectual property, should be viewed through the lens of the international law of transboundary harm—what I will call transboundary cyberharm. Drawing on this doctrine, this Note demonstrates that states have an obligation of due diligence to prevent significant transboundary cyberharm to another state's intellectual property. Second, this Note argues that upon a state's breach of this obligation, affected states may be entitled to reciprocate by neglecting their own due diligence obligation, and allowing their victimized nationals to hack*back*. By understanding private

---

Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 NAVAL L. REV. 132 (2005); COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999) [hereinafter Schmitt, *Normative Framework*]. In 2009, the U.S. National Research Council, an independent organization in Washington, D.C., released a particularly exhaustive report on the use of cyberattack methods by the United States and foreign governments. *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens et al. eds., 2009) [hereinafter NRC Report]. On September 18, 2012, then-State Department Legal Adviser Harold Koh, in a speech before a conference sponsored by United States Cyber Command (USCYBERCOM), outlined the U.S. positions on how the laws of war may apply to cyberspace. *See* Harold Hongju Koh, *International Law In Cyberspace*, 54 HARV. INT'L L.J. ONLINE 1 (2012). Not more than a month prior to Koh's remarks, NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) released a draft of the so-called "Tallinn Manual," the product of a three-year project to apply the laws of war to cyberspace. *See* THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt et al. eds., 2013). For an analysis comparing Koh's remarks to *The Tallinn Manual*, see Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. 13 (2012).

19. *But see* Hannah Lobel, Note, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617 (2012) (examining possible implications under the law of armed conflict for non-state actors). Most other scholarship has discussed the domestic law contours of cyber self-help. *See, e.g.*, Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171 (2005); Zach West, Note, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119 (2012) (arguing for deputation of private companies under the Computer Fraud and Abuse Act to deter cybercrime).

cyber conflict within these traditional international legal principles, this Note brings clarity to the otherwise murky waters of the international law of cyber conflict.

In order to make this case, Part I provides a general overview of the state of hacking and cyber self-defense, paying particular attention to the unique decentralized nature of the Internet. Part II then presents the traditional principles of transboundary harm in international law, showing how these principles can apply in the context of cyber conflict. Part III then explores the framework of decentralized enforcement in international law, arguing that when a state fails to fulfill its due diligence obligation to prevent transboundary cyber-harm, states are permitted to reciprocate through "tailored neglect" of their own due diligence obligation.

I. THREAT AND RESPONSE IN THE DECENTRALIZED SYSTEM

There are more than 2.4 billion Internet users in the world[20]—more than one-third of the global population.[21] The technological advances that have led to greater interconnectedness and wider computer use have greatly increased the ease of controlling aspects of our lives,[22] and are inextricably linked to future economic growth.[23] But this widespread interconnectedness, within the decentralized world of cyberspace, is not without costs. Increased access to this network has also led to increased threats online, with recent documented attacks in the United States by foreign governments,[24] by insurgent groups

20. Internet World Stats, Usage and Population Statistics, *Internet Users in the World*, http://www.internetworldstats.com/stats.htm (last visited Sept. 20, 2013).

21. United Nations Population Fund, *By Choice, Not by Chance: Family Planning, Human Rights and Development*, 17 (Nov. 14, 2012), http://www.unfpa.org/webdav/site/global/shared/swp/2012/EN_SWOP2012_Report.pdf.

22. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 71, 85 (2010).

23. *See generally*, Organization for Economic Co-Operation and Development, Public Affairs Division, *Policy Brief: The Future of the Internet Economy* (2008), *available at* http://www.oecd.org/sti/ieconomy/40780975.pdf.

24. *See, e.g.*, MANDIANT REPORT, *supra* note 2 (discussing the attacks orchestrated by APT1 within the Chinese military); Mark Clayton, *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, CHRISTIAN SCI. MONITOR (Feb. 27, 2013), http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage (reporting cyberattacks on American natural gas pipelines, and citing U.S. suspicions of Chinese military involvement); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (examining cyberattacks against the Georgian State immediately

and other non-state actors,[25] and by so-called "hacktivists."[26] In this Part, I provide a general orientation to the state of hacking, surveying the existing threats in cyberspace, and the available tools to private actors to respond to these threats.

A. "Peacock on the Windshield"—The Decentralized System of the Internet

In 1997, William Cheswick and Hal Burch started the Internet Mapping Project at Bell Labs.[27] By collecting and analyzing the routing paths from a test host to thousands of registered hosts on the Internet, Burch and Cheswick plotted a "map" of the Internet.[28] They named one of their first colorful maps,[29] taken from data in September 1998, the "Peacock on the Windshield," as it depicted a wildly decentralized (and colorful) web with no clear structure and no obvious center.[30]

Since Burch and Cheswick's first map, the Internet has grown at exponential rates, and its structure has not become any more centralized.[31] As of July 2012, there are now more than 908 million

---

prior to the Georgia-Russia conflict in 2008); Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (discussing distributed denial of service attacks against U.S. banks attributed to the Iranian government); *see also* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97 (2010).

25. Siobhan Gorman, Yochi J. Dreazen & August Cole, *Insurgents Hack U.S. Drones*, WALL ST. J., Dec. 17, 2009, http://online.wsj.com/article/SB126102247889095011.html.

26. For example, Anonymous, one of most high-profile of such groups, has reportedly hacked into the computer systems of both the Federal Bureau of Investigation and Scotland Yard. *See* Mark Clayton, *How Did Anonymous Hackers Eavesdrop on FBI and Scotland Yard?*, CHRISTIAN SCI. MONITOR (Feb. 3, 2012), http://www.csmonitor.com/USA/2012/0203/How-did-Anonymous-hackers-eavesdrop-on-FBI-and-Scotland-Yard.

27. *See* Bill Cheswick, Hal Burch & Steve Branigan, *Mapping and Visualizing the Internet*, USENIX Annual Technical Conference (2000).

28. *Id.*

29. *Id.* The maps could be colored in a variety of ways in order to show different data such as IP addresses, domain information, or location.

30. *Id.*; *see also* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 29 (2009).

31. Some readers may dispute the latter of these claims. It is true that the Internet is more centralized in some states than others. *See infra* Part II.B.1 (describing the variance in the exercise of control over the Internet). The overarching claim, however, that there is no

hosts connected to the Internet.[32] These millions of hosts are connected to each other through what is essentially a very large network,[33] governed by a suite of software protocols commonly referred to collectively as TCP/IP.[34] Through these protocols, information can be sliced into small "packets" of data and shuttled to and fro from end-users across the globe.[35] This process, commonly known as "packet switching," is an inherently decentralized system in which there is no centralized technical control.[36] Unlike your local office or home network, there is no central server to which all computers must be connected in order to access the network.[37] Aside from the few governance institutions for addressing devices,[38] the Internet is largely ungoverned and ungovernable—a peacock on the windshield.

---

global centralization, remains true to this day.

32. *See* Internet Systems Consortium, *Internet Domain Survey* (July 2012), http://ftp.isc.org/www/survey/reports/current/.

33. To be precise, the Internet is a network of networks, or an "inter-network." *See* POST, *supra* note 30, at 25; COMM. ON THE INTERNET IN THE EVOLVING INFO. INFRASTRUCTURE ET AL., THE INTERNET'S COMING OF AGE 107–24 (2001) (describing the Internet as "a set of independent networks interlinked to provide the appearance of a single, uniformed network.").

34. *See* LAWRENCE LESSIG, CODE VERSION 2.0, 43 (2006). The acronym is short for "Transmission Control Protocol" (TCP) and Internet Protocol (IP). *Id.*

35. *Id.* ("Brutally simplified, the system takes a bunch of data (a file, for example), chops it up into packets, and slaps on the address to which the packet is to be sent and the address from which it is sent.").

36. *See* ED KROL, THE WHOLE INTERNET: USER'S GUIDE AND CATALOG 13–14 (1992).

37. *See* POST, *supra* note 30, at 29.

38. The Internet Corporation for Assigned Names and Numbers (ICANN) is a nominally nongovernmental organization responsible for the naming and numbering of Internet addresses. *See generally Internet Corporation for Assigned Names and Numbers: Welcome to ICANN!*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org/en/about/welcome/ (last visited Sept. 17, 2013). ICANN has its own complicated and disputatious history. *See also* Stefan Bechtold, *Governance in Namespaces*, 36 LOY. L.A. L. REV. 1239 (2003); Tamar Frankel, *Governing by Negotiation: The Internet Naming System*, 12 CARDOZO J. INT'L & COMP. L. 449 (2004); Tamar Frankel, *The Managing Lawmaker in Cyberspace: A Power Model*, 27 BROOK. J. INT'L L. 859 (2002); A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 47–48 (2000); Viktor Mayer-Schönberger & Malte Ziewitz, *Jefferson Rebuffed: The United States and the Future of Internet Governance*, 8 COLUM. SCI. & TECH. L. REV. 188 (2007); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000) (criticizing the lack of oversight and representation of ICANN); *infra* notes 52–53 on efforts to internationalize ICANN's control. *See generally* MILTON L. MUELLER, RULING THE ROOT 163–226 (2002).

But this decentralization is not due to lack of design or foresight.[39] Proponents hail this seemingly chaotic architecture as the foundation to the Internet's early and continuing success.[40] Commonly referred to as the "end-to-end" principle, the architecture allows for efficiency, ensuring that transportation protocols focus only on the transmission of data,[41] as well as providing flexibility and user choice,[42] being open to almost any sort of device or application. As Tim Wu has argued, this end-to-end principle is "one of the most important reasons that the Internet produced the innovation and growth that it has enjoyed."[43]

At the same time, this decentralization is not without drawbacks. First, while ease of access helps to universalize the benefits of the Internet, it also provides easier access to those who may wish to misuse the Internet for pernicious purposes.[44] The complicated web of interconnected networks, with little oversight or policing, means devastating threats can spread rapidly.[45] For example, the so-called

39. *Cf.* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 266 (2011) (noting that "the Internet abdicates control to the individual; that is its special allure, its power to be endlessly surprising, as well as its founding principle.").

40. Jerome H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS IN COMPUTER SYS. 277 (1984); *see* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 60, 67–100 (2008) ("[I]f the Internet had been designed with security as its centerpiece, it would never have achieved the kind of success it was enjoying . . ."); Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783 (2002) (arguing the end-to-end principle makes the Internet a "commons"); Tim Wu & Christopher Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575 (2007); Lawrence Lessig, *May the Source Be With You*, WIRED (Sept. 12, 2004), http://www.wired.com/wired/archive/9.12/lessig_pr.html; Letter from Condoleezza Rice, U.S. Sec'y of State, to Jack Straw MP, Sec'y of State for Foreign and Commonwealth Aff., U.K. (Nov. 7 2005), *available at* http://it.slashdot.org/story/05/12/ 04/1624219/the-letter-that -won-us-internet-control ("[t]he success of the Internet lies in its inherently decentralized nature"); *see generally* POST, *supra* note 30.

41. In this respect the end-to-end principle implies a "dumb" or "neutral" network. This principle, that the Internet does not favor one application over another, underlies the central debate over "net neutrality." *See* Wu & Yoo, *supra* note 40; Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2005).

42. Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2030 (2006) ("According to end-to-end theory, placing control and intelligence at the edges of a network maximizes network flexibility and user choice.").

43. Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 681 (2003).

44. *See* Zittrain, *supra* note 42, at 2030–31 (discussing the effect of decentralized governance on cybersecurity).

45. For example, one of the fastest computer worms in history, the so-called "Slammer/Sapphire" worm, doubled in size every 8.5 seconds, infecting "more than 90 percent of vulnerable hosts within 10 minutes." *See* David Moore et al., *The Spread of the*

"I Love You" worm that originated in the Philippines caused more than eleven billion dollars in damages in the United States.[46]

International efforts to address Internet governance have been largely tepid or focused on other priorities. In 1998, the Russian Federation proposed a treaty to ban cyber weapons,[47] but the proposal met with a poor response from U.N. Member States.[48] In 2001, the Council of Europe adopted a Cybercrime Convention,[49] which attempted to reconcile domestic definitions of cybercrime,[50] as well as increase cooperation, but it has not gained widespread adoption and some critics consider efforts to cooperate doomed to fail.[51] At the United Nations World Summit on the Information Society (WSIS), a two-stage summit in 2003 and 2005, some states suggested an international government should govern the Internet,[52] but the summit's

---

Sapphire/Slammer Worm, COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS, *available at* http://www.caida.org/outreach/papers/2003/sapphire/index.xml; John Schwartz, *Rampant Epidemics of Powerful Malicious Software*, N.Y. TIMES (Dec. 1, 2003), http://www.nytimes.com/2003/12/01/technology/technology-media-rampant-epidemics-of-powerful-malicious-software.html; John Schwartz, *Worm Hits Microsoft, Which Ignored Own Advice*, N.Y. TIMES (Jan. 28, 2003), http://www.nytimes.com/2003/01/28/technology/28SOFT.html. The SoBig.F virus in 2003 accounted for more than two-thirds of the e-mail traffic in the world. *See* Brendan I. Koerner, *In Computer Security, a Bigger Reason To Squirm*, N.Y. TIMES (Sept. 7, 2003), http://www.nytimes.com/2003/09/07/business/business-in-computer-security-a-bigger-reason-to-squirm.html?pagewanted=all&src=pm; *Sobig is biggest virus of all*, BBC NEWS, Aug. 21, 2003, http://news.bbc.co.uk/2/hi/technology/3169573.stm.

46. *Love Bug Virus Case Dropped in Philippines; No Legal Grounds for Trial of Student*, WASH. POST, Aug. 22, 2000, at A12; *see also infra* Part I.B. (surveying the variety of online threats).

47. Permanent Representative of the Russian Federation to the U.N., Letter dated Sept. 23, 1998 from the Permanent Representative of the Russian Federation to the U.N. addressed to the Secretary-General, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998).

48. Only Cuba and Belarus supported any further development of a proposal. *See* U.N. Secretary-General, Developments in the Field of Information and Telecommunications in the Context of Information Security: Rep. of the Secretary-General, U.N. Doc. A/54/213 (Aug. 10, 1999).

49. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

50. *Id.* arts. 2–13. But as Jack Goldsmith has pointed out, the Convention is weak on enforcement, as it does not permit states to engage in cross-border searches, "even in cases of emergency or hot pursuit." Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 107 (2001).

51. *See, e.g.*, Jack L. Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Peter Berkowitz ed., 2011), *available at* http://www.hoover.org/taskforces/national-security/challenges.

52. *World Summit on the Information Society*, INT'L TELECOMM. UNION, http://www.itu.int/wsis/index.html (last visited Sept. 13, 2013); *Don't Sidetrack ICANN Is Business*

tangible output focused far more on building access and bridging the digital divide than on centralizing governance.[53]

Even if some governance structure were established, the decentralized nature and anonymity of the Internet makes attribution of online threats challenging, requiring identification of not only the computer used but also its operator.[54] The current packet architecture of the core TCP/IP protocols does not provide an authentication mechanism for individual packets,[55] making it nearly impossible to verify a sender's identity.[56] Some have proposed redesigning packet architecture to provide sourcing data for every piece of data.[57] But this restructuring of Internet governance comes with costs. Privacy

---

Plea, INT'L CHAMBER OF COMMERCE (July 10, 2003), http://www.iccwbo.org/News/Articles/2003/Don-t-sidetrack-ICANN-is-business-plea/; ICANN, *At Large Advisory Committee's Statement on WSIS Declaration of Principles and Plan of Actions*, Jan. 20, 2004, *available at* http://atlarge.icann.org/wsis/statement-wsis-20jan04.htm; Kieren McCarthy, *Will December Make or Break the Internet?*, THE REGISTER (Nov. 24, 2003), http://www.theregister.co.uk/2003/11/24/will_december_make_or_break/; INT'L CHAMBER OF COMMERCE, ISSUES PAPER ON INTERNET GOVERNANCE (2004), *available at* http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2004/ICC-Issues-Paper-on-Internet-Governance/.

53. *See* World Summit on the Information Society, *Basic Information: About WSIS*, INT'L TELECOMM. UNION, http://www.itu.int/wsis/basic/about.html (last visited Sept. 13, 2013); John Markoff, *Control the Internet? A Futile Pursuit, Some Say*, N.Y. TIMES (Nov. 14, 2005), http://www.nytimes.com/2005/11/14/business/14register.html; Victoria Shannon, *Other Nations Hope to Loosen U.S. Grip on Internet*, N.Y. TIMES (Nov. 15, 2005), http://www.nytimes.com/2005/11/15/technology/15net.html.

54. CLARKE & KNAKE, *supra* note 22, at 214–15. There have been significant steps forward, however, and attribution, at least at the country level, is not an insurmountable challenge, *see infra* notes 209–210 and accompanying text.

55. Chris Chambers et al., *TCP/IP Security* § 3.2, LINUXSECURITY.COM, http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html (last visited Sept. 13, 2013).

56. NRC Report, *supra* note 18, at 115–16.

57. *See* CLARKE & KNAKE, *supra* note 22, at 274–75; *see also* JEFFREY HUNKER, CREEPING FAILURE: HOW WE BROKE THE INTERNET AND WHAT WE CAN DO TO FIX IT 207 (2010); Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (arguing that the Internet should be reengineered to "make attribution, geolocation, intelligence analysis and impact assessment . . . more manageable"); STUART BIEGEL, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 255–57 (2001); U.S. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 113–18 (2003), *available at* http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; *see also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 404, 438 (2006).

advocates have responded to such proposals militantly,[58] and greater ease of packet attribution may make it easier for authoritarian regimes to censor speech, such as in China.[59] Indeed, following the recent disclosure about surveillance programs by the National Security Agency (NSA), reports emerged that administrative officials viewed a national cyber defense program as politically infeasible.[60] Even if such redesign were practicable,[61] Jonathan Zittrain has argued that measures such as packet identification would undermine the very "generativity" of the Internet's decentralized architecture.[62]

B. The Threat—Cyberharm, Attack, and Exploitation

In part because of the Internet's decentralized architecture, which allows for ease of access as well as anonymity, the potential for malicious attacks against governments, as well as private firms, is a natural side effect.[63] The growing use of "cloud computing" and mobile devices only increases these risks.[64] In 2012, an annual study of fifty-six large American firms found that they incurred more than a hundred cyber attacks a week in that year alone, a forty-two percent rise from the previous year.[65] But there is tremendous variety in the types of cyber attacks,[66] each with different goals, purposes, and ef-

58. Paul Van Slambrouck, *New Computer Chip: Useful Tool or Privacy Invasion?*, CHRISTIAN SCI. MONITOR, Feb. 16, 1999, http://www.csmonitor.com/1999/0216/p2s2.html.

59. *See generally* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert et al. eds., 2008).

60. David E. Sanger, *N.S.A. Leaks Make Plan for Cyberdefense Unlikely*, N.Y. TIMES (Aug. 12, 2013), http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html (reporting a senior intelligence official as saying "[w]hatever trust was there is now gone. . . . I mean, who would believe the N.S.A. when it insists it is blocking Chinese attacks but not using the same technology to read your e-mail?").

61. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 598–99 (2011) (arguing packet redesign is a practically difficult, if not impossible task, demanding the consensus of interested parties).

62. *See* Zittrain, *supra* note 42, at 2030–31 (2006); *see also supra* note 40 and accompanying text.

63. *See supra* notes 44–46 and accompanying text.

64. *See* ECONOMIST, *Firewalls and Firefights*, *supra* note 11.

65. *See Computer Hacking: A byte for a byte*, ECONOMIST (Aug. 10, 2013), http://www.economist.com/news/leaders/21583268-letting-companies-strike-back-computer-hackers-bad-idea-byte-byte.

66. According to a report by the National Research Council, cyberattack refers to actions to "alter, disrupt, deceive, degrade, or destroy adversary computer systems or

fects. While some seek to disrupt or damage a target computer system, others seek instead to rob a system of information.

1. Distributed Denial of Service (DDoS) Attacks

Distributed denial-of-service (DDoS) attacks, one of the most basic forms of attack, typically utilize large numbers of "zombie" computers to systematically bombard a given target.[67] These zombie computers, forming so-called "botnets," often number in the millions of computers, and repeatedly request access to a target, overwhelming the network and denying service to genuine end-users. For example, in July 2009, a DDoS attack against the United States and South Korea, which some attributed to North Korea,[68] was launched from computers in at least six countries, including the United States.[69] The attack affected the Web sites of the U.S. Secret Service and South Korea's presidential Blue House, among others.[70]

In 2007, Estonia's foreign and justice ministries, along with its two largest banks, were nearly paralyzed by a systematic and orchestrated cyber attack,[71] which also hit members of the Estonian parliament as well as several news organizations.[72] Functionally, the

---

networks or the information and/or programs resident in our transiting these systems or networks." NRC Report, *supra* note 18, at 80; *see also* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 63 (2010).

67. Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 245 n.41 (2003).

68. *Pentagon Official: North Korea Behind Week of Cyber Attacks*, FOX NEWS (July 9, 2009), http://www.foxnews.com/story/2009/07/09/pentagon-official-north-korea-behind-week-cyber-attacks/. *But see* Lolita C. Baldor, *U.S. Largely Ruling out North Korea in 2009 Cyber Attacks*, USA TODAY (July 6, 2010), http://usatoday30.usatoday.com/tech/news/computersecurity/2010-07-06-nkorea-cyber-attacks_N.htm.

69. D.J. Walker-Morgan, *DDoS Attacks with Zombie Computers—'North Korea's Powerful Hacker Army'?*, THE H SECURITY (July 10, 2009), http://www.h-online.com/security/news/item/DDoS-attacks-with-zombie-computers-North-Korea-s-powerful-hacker-army-742435.html.

70. Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea*, N.Y. TIMES (July 8, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html.

71. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 2007), http://www.theguardian.com/world/2007/may/17/topstories3.russia.

72. Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, 9 EUR. AFF. nn.1–2, at 20 (2008); *Estonia and Russia: A Cyber-Riot*, ECONOMIST (May 10, 2007), http://www.economist.com/node/9163598.

attack was a DDoS attack,[73] using an estimated one million zombie computers commandeered by the attackers to systematically disrupt the Estonian cyber infrastructure.[74] Although the attack did not cause significant economic harm or any physical damage,[75] it disrupted the Estonian economy for a substantial period of time, and was widely suspected to be in retaliation for Estonia's removal of a statue honoring the Soviet Union's role in World War II.[76]

2. Malicious Software Attacks

While DDoS attacks can be somewhat effective, they are largely a simplistic mechanism that merely denies access for a temporary period of time. Malicious software, or malware, on the other hand, can be significantly more complex.[77] These attacks exploit a vulnerability in a computer system to gain access and then execute a "payload" into that system to achieve a particular goal or set of goals.[78] Early malware traditionally took the form of viruses or worms.[79] Viruses, much like their biological analog, are merely fragments of code that are capable of copying themselves into other programs, and altering their code to carry out a given purpose.[80] By contrast, worms are stand-alone programs and can carry out more complicated tasks while spreading at remarkable speeds.[81]

The most high-profile and successful cyber attack of this nature to date was the famed "Stuxnet" worm. Stuxnet, first discov-

---

73. DDoS attacks commonly involve "commandeering the computers of unsuspecting users and using these distributed systems, referred to as 'zombies,' to flood a particular website or service provider with junk messages." Lipton, *supra* note 67.

74. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html.

75. *See id.*; Ruus, *supra* note 72.

76. Traynor, *supra* note 71; *see also* CLARKE & KNAKE, *supra* note 22.

77. These can take "a wide variety of forms, including Trojan horses, rootkits, exploits, and 'zombies.'" Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 442 (2011).

78. NRC Report, *supra* note 18, at 83.

79. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 14 (2009).

80. *Id.* at 14–15.

81. *Id.*; *see also supra* note 45.

ered by a computer security firm in Belarus,[82] is largely credited for causing severe damage to an Iranian nuclear enrichment facility in 2010.[83] According to news reports, the worm, which was jointly orchestrated by American and Israeli intelligence,[84] set back Iran's nuclear weapons program by at least three years.[85]

3. Advanced Persistent Threats

While DDoS and malware seek to disrupt or otherwise cause damage to a target's network or underlying infrastructure, other forms of cyberharm, potentially even more damaging, exploit vulnerabilities in a target's computer system to obtain information that would otherwise be kept confidential.[86] While these forms of cyberharm may utilize malicious software, their ultimate goal is to gather information from the target computer system, not to disrupt or damage it. When engineered by sophisticated actors, Advanced Persistent Threats (APTs)[87] can be devastatingly successful.[88]

---

82. Gregg Keizer, *Is Stuxnet the 'best' malware ever?*, COMPUTERWORLD (Sept. 16, 2010), http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.

83. *See* Mark Clayton, *Stuxnet Attack on Iran Nuclear Program Came About a Year Ago, Report Says*, CHRISTIAN SCI. MONITOR, Jan. 3, 2011, at 3. The worm reportedly functioned by causing Iran's uranium enrichment centrifuges to spin at too fast a rate, destroying some of the machines, while sending reports back to Iranian engineers monitoring them painting a false picture of normal operation. *See* Christopher Williams, *Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'*, DAILY TELEGRAPH (Jan. 21, 2011), http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html; *see also* William J. Broad, *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 15, 2011, at A1; Kim Zetter, *Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant*, WIRED (Feb. 11, 2011), http://www.wired.com/threatlevel/2011/02/stuxnet-five-main-target/.

84. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

85. Broad, *supra* note 83.

86. Lin, *supra* note 66, at 63; *see also* NRC Report, *supra* note 18, at 19.

87. APTs are *advanced* because of their frequent use of sophisticated intrusion technologies and techniques. *See* DAMBALLA, INC., WHAT'S AN APT? A BRIEF DEFINITION (2010), *available at* https://www.damballa.com/knowledge/advanced-persistent-threats.php. They are *persistent* because their long-term strategy is focused on surreptitious intrusion, through slow progress. *Id.*; *see also infra* note 95 and accompanying text. Finally, they are a *threat* because the intrusion is directed by sophisticated, "motivated, organized and well funded" operators. *Id.*

88. In the terminology of the NRC Report, this might more readily be classified as "cyberexploitation" as it does not cause any direct destruction. Hostile actions taken against

For example, in 2009, Coca-Cola Co. was pursuing the acquisition of the China Huiyan Juice Group for $2.4 billion, which at the time would have been the largest foreign takeover of a Chinese company.[89] On March 15, 2009, the FBI informed Coca-Cola that hackers traced back to China had obtained confidential files concerning the attempted acquisition.[90] Three days later, the deal fell apart, which many attributed to the exposure of confidential materials pertaining to the proposed deal.[91]

To gain a foothold in target networks, APTs typically utilize "spear phishing" techniques.[92] Spear phishing often begins with e-mails to an individual inside a target organization.[93] The e-mail will appear both benign and familiar, frequently containing an attachment masquerading as something related to that individual or the business.[94] When the target opens the attachment, however, the malicious file will infect the target network, surreptitiously building a back door through which the intruders will be able to continually peer inside the organization's system.[95] Once the intruder has established a foothold through the back door, it can then continue to acquire confidential information, such as usernames and passwords, to gain more and more access to a private network.[96]

C. The Response—Passive and Active Defense

Threats, clearly, are aplenty in cyberspace. But the Internet has more-or-less coped with these threats by constantly and consistently playing catch-up with the thieves, culprits and hooligans. Much

---

computer systems can also take the form of non-destructive "exploitation" in order to extract information that would otherwise be confidential. *See* Lin, *supra* note 66, at 63.

89. Ben Elgin, Dune Lawrence & Michael Riley, *Coke Gets Hacked And Doesn't Tell Anyone*, BLOOMBERG (Nov. 4, 2012), http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html; *see also* Nicole Perlroth, *Study May Offer Insight Into Coca-Cola Breach*, N.Y. TIMES BITS BLOG (Nov. 30, 2012), http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/.

90. *See* Elgin et al., *supra* note 89. Analysts attributed the intrusion to Comment Crew. *Id.*

91. *Id.*

92. *See* MANDIANT REPORT, *supra* note 2, at 28.

93. *Id.*

94. *Id.*

95. *Id.* at 28–30. For example, APT1 might send an e-mail to a target with what appears to be a benign Adobe PDF file with a germane title. *Id.* at 30.

96. *Id.* at 34.

of the effort, however, has focused on *passive* defense mechanisms. These cybersecurity methods seek to block or catch threats before they can cause significant harm. However, as threats have become more advanced, the public and private sectors have begun to explore *active* defense methods, to proactively counterattack intruders to disrupt or disable the threat.

1. Methods of Response

In addition to basic and passive cybersecurity measures such as firewalls, other more active cybersecurity methods are often utilized to delude or otherwise derail an attempted threat. For example, a network may construct a number of "tarpits" or computer entities designed to intentionally respond slowly.[97] By slowing the progress of a cyber threat, tarpits serve not only to delay the impact of threats, but also to provide time needed to identify the intruders.[98] Similarly, network engineers can build "honeypots" or traps that appear desirable to an intruder, but enable the system to capture information critical to determining the source of the intrusion.[99]

Absent active defense, firms are largely limited to detection software, firewalls, and other defensive methods.[100] But in response to more sophisticated threats, firms have developed even more aggressive defense measures to respond to threats of growing severity and complexity.[101] A number of startups—such as CrowdStrike,

97. Laurent Oudot & Thorsten Holz, *Defeating Honeypots: Network Issues, Part 1*, SYMANTEC (Sept. 27, 2004), http://www.symantec.com/connect/articles/defeating-honeypots-network-issues-part-1 (updated Nov. 2, 2010).

98. For example, Mykonos Software uses tarpits for clients to detect and distract intruders, "slowing progress as they unwittingly reveal information that can be used to stop, identify or prosecute them." James Temple, *Hackers Getting Hacked by Security Firms*, SFGATE (Nov. 30, 2011), http://www.sfgate.com/business/article/Hackers-getting-hacked-by-security-firms-2306472.php#page-1.

99. LANCE SPITZNER, HONEYPOTS: TRACKING HACKERS 23 (2003).

100. Jay P. Kesan & Ruperto Majuca, *Optimal Hackback*, 84 CHI.-KENT L. REV. 831, 834–35 (2010). One alternative, though limited in application, may be insuring against risk by purchasing cyber liability insurance. *Cf.* Wendy S. Meyer, *Insurance Coverage for Potential Liability Arising from Internet Privacy Issues*, 28 J. CORP. L. 335, 342–43 (2003); *see also* NRC Report, *supra* note 18, at 64 n.26.

101. *See, e.g.*, Joseph Menn, *Hacked companies fight back with controversial steps*, REUTERS (June 17, 2012), http://www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617; ECONOMIST, *Firewalls and firefights*, *supra* note 11. It is difficult to determine to what extent these active defense measures are prevalent. Aside from Google, few firms have disclosed any particular attempts at hacking back. *See supra* notes 7–10 and accompanying text. Even for firms who may be pursuing

Endgame, and CloudFare—have attracted significant investment, promising technology to actively defend corporations against online threats.[102] Though these active defense measures appear to be a recent innovation, especially by private actors, retaliatory action has existed for some time. In 1998, when a hacktivist group launched a DDoS attack against the Pentagon, the government responded in kind to crash the group's network.[103] In the public sector, "active threat neutralization" is the responsibility of the United States Military.[104] The federal government has provided U.S. Strategic Command (STRATCOM) with the authority to neutralize cyber threats that compromise the mission effectiveness of the U.S. Department of Defense.[105]

In the private sector, active defense may be increasingly important to respond to serious threats. In March 2004, Symbiot, Inc. announced what it called the first security solution that could "plan and execute appropriate countermeasures."[106] The firm provided

---

these options, negative publicity associated with hacking is a strong disincentive for disclosure. The concern that disclosure will negatively impact a firm's financial market position, its reputation or brand, as well as the potential for litigation or liability, incentivizes firms to avoid public disclosure. *See* BRIAN CASHELL ET AL., CONG. RESEARCH SERV., RL32331, THE ECONOMIC IMPACT OF CYBER-ATTACKS 13–14 (2004). Game theoretical approaches suggest that there are circumstances in which aggressive active defense is the optimal response. *See* Kesan & Majuca, *supra* note 100, at 832–33; Curtis E. A. Karnow, *Launch on Warning: Aggressive Defense of Computer Systems*, 7 YALE J.L. & TECH. 87 (2005); Smith, *supra* note 19. Microsoft has begun an experimental approach focused on cybercrime and botnet takedowns. *See, e.g.*, Richard Domingues Boscovich, *Bamital Botnet Takedown Is Successful, Cleanup Underway*, OFFICIAL MICROSOFT BLOG (Feb. 22, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/02/22/bamital-botnet-takedown-is-successful-clean-up-underway.aspx.

102. *See* ECONOMIST, *Firewalls and firefights*, *supra* note 11.

103. *See* Winn Schwartau, *Striking Back: Corporate Vigilantes Go on the Offensive to Hunt Down Hackers*, NETWORK WORLD, Jan. 11, 1999, at 1.

104. NRC Report, *supra* note 18, at 54. Successful direct action requires essentially three elements: detection, identification and effective response. *Cf.* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 481 (2012) (Identifying the three elements as "an intrusion detection system . . . the ability to trace an attack back to its origin . . . and then a method of response."). The technical aspects of each of these elements are complicated.

105. NRC Report, *supra* note 18, at 63.

106. *Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers; Aggressive New Rules of Engagement Established in "Information Warfare"*, BUS. WIRE (Mar. 4, 2004), http://www.businesswire.com/news/home/20040304005627/en/Symbiot-Security-Announces-Worlds-Solution-Strike-Network-Based.

several models for such hackbacks, including accessing, disabling, or destroying the hacker's assets, exploiting the vulnerabilities of an attacker's system, even offering retaliatory and disproportionate counterstrikes.[107]

2. The Costs and Benefits of Hacking Back

Hackbacks avoid some of the most troublesome challenges of traditional remedies, including "lengthy prosecutions, thorny jurisdictional matters, technologically unsophisticated juries, and slow courts,"[108] which are unhelpful when viruses and worms can propagate at remarkable speeds.[109] Traditional law enforcement typically lacks the resources or the expertise to adequately respond to cyber attacks,[110] and is largely ineffective in cases of cross-border intrusions.[111] Firms may also be unwilling to publicly disclose vulnerabilities, for fear that disclosure of cybersecurity weaknesses may negatively affect the firm's stock price,[112] its reputation or brand,[113]

---

107. West, *supra* note 19, at 131; *see* Smith, *supra* note 19, at 172.

108. Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 60 (2005).

109. For example, the devastating Sapphire/Slammer worm doubled in size every eight and a half seconds. Moore et al., *supra* note 45.

110. Karnow, *supra* note 101.

111. *See generally* Goldsmith, *supra* note 50 (discussing the limits of cross-border enforcement, though arguing for the legality of more aggressive cross-border investigation). In one particularly high-profile example of successful enforcement actions taken against foreign threats, the FBI traced hackers, who had targeted banks and other firms in the United States, to servers in Russia. *Id.* at 103. The FBI agents then lured the hackers to the United States, where they were apprehended and charged. Robert Lemos, *Lawyers Slam FBI 'Hack'*, ZDNET NEWS (May 2, 2001), http://www.zdnet.com/lawyers-slam-fbi-hack-20212 00883/; Allison Linn, *FBI's Elaborate Hacker Sting Pays Off: High-Tech Gambit Nets 2 Russians*, CHI. TRIB., May 10, 2001, at 20. One of the hackers was later found guilty of a number of charges. Michelle Delio, *'Stung' Russian Hacker Guilty*, WIRED (Oct 17, 2001), http://www.wired.com/politics/law/news/2001/10/47650.

112. *See* Katherine Campbell et al., *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUTER SEC. 431 (2003).

113. *See* BRIAN CASHELL ET AL., *supra* note 101, at 10, 15 (noting that disclosure will negatively impact a firm's financial market position, its reputation or brand, as well as the potential for litigation or liability, which may incentivize firms to avoid public disclosure); *see also* Nicole Perlroth, *Some Victims of Online Hacking Edge Into the Light*, N.Y. TIMES, Feb. 20, 2013, at A1 (noting that despite the widespread compromises, there are few admissions and that a "majority of companies that have at one time or another been the subject of news reports of online attacks refuse to confirm them . . . includ[ing] the International Olympic Committee, Exxon Mobil, Baker Hughes, Royal Dutch Shell, BP,

or that competitors could use disclosed vulnerabilities to their advantage.[114] Simply put, we might favor hackbacks because there currently is no better method to enforce cyberspace violations.[115] Traditional police investigations may take too much time to respond to the swift threat that a malicious cyber attack may pose to an organization.[116] Active defense measures, by contrast, can respond rapidly and may significantly drive up the costs that hackers incur, deterring future conduct.[117]

That said, some have argued that counterstrikes would be unjust, amounting to guilt without a fair trial.[118] Neal Katyal has argued that self-help responses may raise distributional concerns by not protecting those who need it the most and fragmenting communities.[119] Katyal and others also worry about the risk of counterstrikes missing their target and hitting innocent third parties.[120] Indeed, zombie computers in a DDoS botnet may be "operated by hospitals, governmental units, and telecommunications entities."[121] In this cir-

---

ConocoPhillips, Chesapeake Energy, the British energy giant BG Group, the steel maker ArcelorMittal and Coca-Cola.").

114. *See* LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INST., 2004 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 14 (2004), *available at* http://www.infragardphl.org/resources/FBI2004.pdf. In October 2011, the U.S. Securities and Exchange Commission issued guidelines directing publicly traded companies to disclose hacking incidents. *See* U.S. SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. The document, however, issued in the form of agency guidance, is not a binding rule on firms. *See* Joseph Menn, *SEC Issues Guidelines on Hacking*, FIN. TIMES (Oct. 14, 2011), http://www.ft.com/intl/cms/s/0/32e2adae-f5fc-11e0-bcc2-00144feab49a.html. We might (validly) worry that this is a reason to be wary of self-help, and that greater access to these remedies would only encourage greater secrecy.

115. Karnow, *supra* note 101, at 89; *cf.* Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J.L. ECON. & POL'Y 1, 26 (2005) (arguing that self-help can fill the vacuum left by judicial remedies that are too slow or ill equipped to respond).

116. Kesan & Majuca, *supra* note 100, at 834.

117. *See, e.g.*, RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 242 (5th ed. 1998) ("The model can be very simple: A person commits a crime because the expected benefits of the crime to him exceed the expected costs."); ECONOMIST, *Firewalls and Firefights*, *supra* note 11 (quoting an expert in active defense mechanisms as saying the "goal of all these technologies is to drive up the costs that hackers incur in the hope this will deter them in future. It is not to wreak havoc in enemy servers.").

118. *See, e.g.*, Bruce Schneier, *Counterattack*, CRYPTO-GRAM NEWSLETTER (Dec. 15, 2002), *available at* https://www.schneier.com/crypto-gram-0212.html.

119. Katyal, *supra* note 108, at 61.

120. *Id.* at 62.

121. Karnow, *supra* note 101, at 93.

cumstance, inaccurate or disproportionate responses could have a devastating impact.

In short, self-help remedies are not perfect, but they also cannot be written off. Given the inadequacies of the current legal regime, especially with respect to cross-border intrusions, we can expect private firms to increase their use of active defense measures. The question is not whether they will be used, but how states will regulate their use to best protect the property of their nationals while optimizing the Internet's continuing generativity.

II. THE OBLIGATION TO PREVENT TRANSBOUNDARY CYBERHARM

When Coca-Cola was compromised in 2009,[122] it lost a potential $2.4 billion deal in what would have been the largest foreign acquisition in China. Some of the biggest Fortune Global 2000 firms have been similarly compromised.[123] Though the costs of these exploitations are thought to be significant, the story of the precise costs remains largely untold.[124] But it is well recognized that widespread cyber espionage "undermines the corporate sector's ability to create jobs, generate revenues [and] foster innovation."[125] The puzzle is that despite the significance of the harm, scholars have largely viewed this form of exploitation as virtually unregulated by international law.[126] In part, this may be due to the difficulty in analogizing traditional rules of international law to emerging technologies. Most principles of international law are physical in nature,[127] but the Internet, along with the general development of the service and communications economy,[128] does not fit comfortably within this paradigm.

---

122. *See supra* notes 89–91 and accompanying text.

123. *See* Perlroth, *supra* note 113, at A1.

124. OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE (ONCIX), FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE, Oct. 2011, at 3–4 [hereinafter ONCIX Report] (noting that "[d]ata on the effects of the theft of trade secrets and other sensitive information are incomplete" and that "[e]stimates from academic literature on the losses from economic espionage range so widely as to be meaningless—from $2 billion to $400 billion or more a year—reflecting the scarcity of data and the variety of methods used to calculate losses.").

125. *Id.* at 3.

126. *See supra* note 18 and accompanying text.

127. For example, in international trade law, the traditional conception was the trade of *goods*, such as wheat and wine, traded between two countries. DAVID RICARDO, ON THE PRINCIPLES OF POLITICAL ECONOMY AND TAXATION (1817).

128. *See* Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J.

As a result, analogies made may exclude activities on the Internet altogether from the ambit of international law—in other words, significant cyberharm risks being lost in translation.[129]

This view is mistaken. In this Part, this Note argues that cross-border cyber attacks should be analogized to the traditional principles of transboundary harm. To make this case, this Part first provides a background on the international legal obligation to prevent transboundary harm. It then translates these principles to the context of the Internet, showing that while alternative legal regimes stumble over obstacles such as attribution and state responsibility, principles of transboundary cyberharm avoid such challenges.

A. The International Obligation to Prevent Transboundary Harm

As a corollary to the principles of sovereign equality and territorial sovereignty, international law imposes an obligation on states to prevent significant transboundary harm.[130] The International

---

INT'L L. 263, 266 (2006) (discussing that the architects of international trade law in the 1980s and 1990s did not anticipate the rapid growth of the service and communications sectors).

129. *Cf.* Harold Hongju Koh, Legal Adviser, U.S. Department of State, Remarks at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm (arguing that determining, as a matter of international law, the scope of detention authority in the context of terrorism requires some "'translation,' or analogizing principles from the laws of war governing traditional *international* conflicts."). The traditional metaphor of the Internet has been to liken cyberspace to a physical place. *See generally* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003). For example, this metaphor is widely used in U.S. jurisprudence. Courts have likened unauthorized access of computers to common law trespass. *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (holding that excessive and unauthorized e-mail messages were not a trespass-to-chattel because they did not cause an injury to the plaintiff's property). Courts also frequently liken Internet service providers to newspaper publishers or telecommunications carriers. *See* Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 474 (citing Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995); Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)). This approach, however, has been routinely criticized. *See, e.g.*, Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J. L. ECON. & POL'Y 197 (2005) (arguing that imagining cyberspace as a virtual world with physical processes carries with it assumptions with regard to the limits, practices, and rules of the physical world).

130. Though much of this law is treaty-based, customary international law remains an important source of the international law relating to transboundary harm, environmental or otherwise. *See* Pierre-Marie Dupuy, *Overview of the Existing Customary Legal Regime*

Court of Justice has declared this obligation, long recognized by common law courts in domestic jurisdictions,[131] as a rule of customary international law.[132] Though this principle is generally accepted, the contours of its requirements are murky.

1. The Principles of Transboundary Harm

The first articulation of the principle of transboundary harm by an international tribunal was the *Trail Smelter* arbitration between the United States and Canada.[133] In *Trail Smelter,* the dispute centered on emissions from smelting plants that crossed into parts of the

---

Regarding International Pollution, in INTERNATIONAL LAW AND POLLUTION 61 (Daniel Barstow Magraw ed., 1991); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 601–04 (1987).

131. Common law courts have espoused for centuries the Roman law principle *sic utere tuo ut alienum non laedas* that "every man must so use his own as not to damnify another." *See, e.g.*, Tenant v. Goldwin, (1704) 92 Eng. Rep. 222, 224 (K.B.). For this reason, it might also be argued that it is a general principle of law. *See* Statute of the International Court of Justice art. 38(1)(c).

132. *See, e.g.*, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 29 (July 8). This is not to suggest that it is not without its detractors. Daniel Bodansky, for example, has strongly questioned the notion that there is a customary duty to prevent transboundary *pollution*, preferring to call the norms "declarative." Daniel Bodansky, *Customary (and Not So Customary) International Environmental Law*, 3 IND. J. GLOBAL LEGAL STUD. 105, 116 (1995). Nonetheless, Bodansky does seem to recognize that the general rule of *Corfu Channel*, that a state may not knowingly allow its territory to be used to harm another state, is part of the general corpus of international law. Commonly, reference is made to Principle 21 of the Stockholm Declaration as an additional signal to the principle's place in international law. The declaration states:

> States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own natural resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction.

United Nations Conference on the Human Environment, Stockholm, Swed., June 5–16, *Report of the United Nations Conference on the Human Environment*, Pt. One, Ch. I, Principle 21, U.N. Doc. A/CONF.48/14/Rev.1 (June 16, 1972) [hereinafter "Stockholm Declaration"]. This principle was later reaffirmed in the 1992 "Rio Declaration." *See* United Nations Conference on Environment and Development, Rio de Janeiro, Braz., June 3–14, 1992, *Rio Declaration on Environment and Development*, Principle 11, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I), Annex I (Aug. 12, 1992) [hereinafter "Rio Declaration"].

133. ANTONIO CASSESE, INTERNATIONAL LAW 484 (2d ed. 2005) (*Trail Smelter* was the first decision by an international tribunal holding that "a State may not use, or allow its nationals to use, its own territory in such a manner as to cause injury to a neighboring country.").

state of Washington, harming crops and fisheries.[134] These activities by the Consolidated Mining and Smelting Company led to an arbitral decision held up as the *locus classicus* of international law on transboundary harm.[135] The tribunal famously held that "no state has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence."[136] Furthermore, the tribunal found Canada to be "responsible in international law for the conduct of the Trail Smelter"[137] and held that it was "the duty of the Government of the Dominion of Canada to see to it that this conduct should be in conformity with the obligation of the Dominion under international law as herein determined."[138]

Though this principle is commonly invoked in the environ-

134. Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1924–33 (1938) (discussing the extent of the damage caused by the fume emissions); *see also* Rebecca M. Bratspies & Russell A. Miller, *Transboundary Harm in International Law: Lessons from the* Trail Smelter *Arbitration*, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 1 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

135. Günther Handl, *Territorial Sovereignty and the Problem of Transnational Pollution*, 69 AM. J. INT'L. L. 50, 60 (1975); *see also* TUOMAS KUOKKANEN, INTERNATIONAL LAW AND THE ENVIRONMENT: VARIATIONS ON A THEME 89 (2002) ("The Trail Smelter case is one of the landmarks of the traditional period to which scholars constantly refer."); JAN SCHNEIDER, WORLD PUBLIC ORDER OF THE ENVIRONMENT: TOWARDS AN INTERNATIONAL ECOLOGICAL LAW AND ORGANIZATION 50 (1979) (describing *Trail Smelter* as a "milestone" in international environmental law); ALEXANDRE KISS & DINAH SHELTON, INTERNATIONAL ENVIRONMENTAL LAW 107 (1991) (describing *Trail Smelter* "as having laid out the foundations of international environmental law, at least regarding transfrontier pollution"); Linda A. Malone, *The Chernobyl Accident: A Case Study in International Law Regulating State Responsibility for Transboundary Nuclear Pollution*, 12 COLUM. J. ENVTL. L. 203, 208 (1987) ("Any analysis of [foreign] liability necessarily begins with the landmark Trail Smelter case."); Thomas W. Merrill, *Golden Rules for Transboundary Pollution*, 46 DUKE L.J. 931, 947 (1997) ("By far the most influential decision on transboundary pollution in international law is the *Trail Smelter* arbitration"); Karin Mickelson, *Rereading Trail Smelter*, 31 CAN. Y.B. INT'L L. 219, 219–20 (1993) (explaining that the *Trail Smelter* arbitration is "more an object of reverence than a subject of analysis" but is "one of the best known and most frequently cited international decisions, and is regarded by many scholars as the fountainhead of modern international environmental law").

136. *Trail Smelter*, 3 R.I.A.A. at 1965. As authority for this holding, the tribunal cited a leading international law scholar at the time, Clyde Eagleton, who wrote, "A State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction." *Id.* at 1963 (quoting CLYDE EAGLETON, RESPONSIBILITY OF STATES IN INTERNATIONAL LAW 80 (1928)) (internal citation omitted).

137. *Trail Smelter*, 3 R.I.A.A. at 1965.

138. *Id.* at 1966.

mental context, it is not so limited. In the *Corfu Channel* case, the ICJ elaborated on *Trail Smelter*, holding that states have a general obligation to prevent transboundary harm to another state's rights.[139] In *Corfu Channel*, the United Kingdom alleged that Albania was responsible for mines in its waters that damaged two of its naval warships in Albanian waters in the Corfu Channel.[140] Notably, however, the Court did not find that the mines had been laid directly by Albania. Dismissing a theory of direct liability,[141] as well as a theory that Albania had colluded with Yugoslavia,[142] the Court found Albania liable by virtue of the mines having been laid with its knowledge.[143] The Court found that Albania's close awareness of activities in the channel during the relevant time period meant that the mines could not have been placed without Albania's knowledge.[144] As a result, the Court held that Albania was responsible for notifying states of the mines, finding that every state had an obligation "not to allow knowingly its territory to be used contrary to the rights of other States."[145]

Most recently, in 2001, the International Law Commission (ILC) recognized these principles as rules of customary international law, adopting the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities.[146] The articles, though not yet formally endorsed by the U.N. General Assembly,[147] represent an at-

139. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9). In the context of *Corfu Channel*, the state's right was the undisputed rule of international law of safe passage through another state's territorial waters in peacetime. *Id.*

140. *Id.*

141. *Id.* at 16.

142. *Id.* at 17.

143. *Id.* at 17–22. Here, the Court first articulated a burden of proof doctrine that was more lenient for a complaining state when the alleged harm took place in an area under the "exclusive territorial control" of the other state. *Id.* at 18. The Court noted that though "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any lawful act perpetrated therein, nor yet that it necessarily knew, or should have known," the exclusive territorial control nonetheless could provide for a lessened threshold for proof for the complaining state. *Id.*

144. *Id.* at 20–22.

145. *Id.* at 22.

146. Report of the Int'l. L. Comm'n., Apr. 23–June 1, July 2–Aug. 10, 2001, U.N. Doc. A/56/10; GAOR, 53rd Sess., Supp. No. 10, art. 3, at 372 (2001) [hereinafter "Draft Articles on Transboundary Harm"].

147. In its latest action in 2010, the U.N. General Assembly commended the draft articles and decided to include consideration of the draft articles in the provisional agenda of its sixty-eighth session in 2013. *See* U.N. Doc. A/RES/65/28 (Jan. 10, 2011).

tempt to codify the customary international law on the subject of transboundary harm.[148] In the commentaries to the articles, the Special Rapporteur noted that the scope of the prohibition was limited to four criteria,[149] each of which is worth discussion.

First, the articles refer to "activities not prohibited by international law."[150] The nuance in this first criterion means to distinguish international liability from state responsibility,[151] a distinction well reflected in the ILC's *Articles on State Responsibility*.[152] As a result, though the state may not be held internationally responsible for the acts *themselves*, it may still have breached an independent obligation to prevent those acts.[153]

Second, the ILC's articles limit the prohibition to activities under the territorial jurisdiction of the state.[154] In this regard, the ILC stressed that "territorial jurisdiction" is the dominant criterion that gives rise to liability.[155] As a result, the obligation of prevention applies to any activity that "occurs within the territory of a State."[156] However, though territory is held as conclusive evidence of jurisdiction, and therefore liability, Article Two of the *Draft Articles on Transboundary Harm* extends the obligation likewise to any area under the jurisdiction or control of the state.[157]

Third, the activities involved regard a "risk of causing significant transboundary harm."[158] This can be unpacked into the two interrelated elements: the risk of harm and threshold magnitude of that

148. *See* Draft Articles on Transboundary Harm, *supra* note 146, at 59–62 (setting out the purpose to codify and develop the international law of prevention of transboundary harm).

149. *Id.* art. 1, cmt. ¶ 5.

150. *Id.* art. 1, cmt. ¶ 6.

151. *Id.*

152. Text of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, in *Report of the Int'l Law Comm'n*, 53rd sess., Apr. 23–June 1, July 2–Aug. 10, 2001, U.N. Doc. A/56/10; U.N. GAOR, 56th Sess. Supp. No. 10, at 43 (Oct. 1, 2001) [hereinafter "Draft Articles on State Responsibility"].

153. As I argue in Part III, this distinction is critically important from the standpoint of remedy. *See infra* Part III.B. Because the international legal obligation breached is one of *prevention of harm*, a state's reciprocal countermeasures are largely limited to a corresponding cessation of their own obligation to prevent harm. *Id.*

154. Draft Articles on Transboundary Harm, *supra* note 146, art. 1, cmt. ¶¶ 7–8.

155. *Id.* art. 1, cmt. ¶ 8.

156. *Id.*

157. *Id.* art. 2(d).

158. *Id.* art. 1, cmt. ¶ 13.

harm. The ILC stated that the risk is a function of the probability of an accident and the "magnitude" of the impact.[159] Thus, if the combined effect of the probability of the harm, and the magnitude of that harm, rise to the level that is deemed "significant," the risk prong has been met.[160] As a result, liability could be imposed for ultrahazardous activities despite a low probability of an accident as well as minimally harmful activities with a very high probability of accidents. Second, the "significance" element, which echoes similar language in the *Trail Smelter* arbitration, requires a fact-intensive inquiry that the Special Rapporteur admitted was "not without ambiguity."[161] At the very least, however, there has to be a "real harm" to, for example, "human health, industry, property, environment or agriculture" in the victim state.[162]

Fourth, the harm must have been caused by the "physical consequences" of the activities.[163] This limitation is intended to remove from the scope of the prohibition any harm caused by state policies with respect to monetary or socio-economic fields.[164] The Special Rapporteur noted that this requirement implies that the activities covered by the articles "must themselves have a physical quality, and the consequences must flow from that quality."[165]

2. The Obligation's Scope: The Due Diligence Principle

It is worth greater discussion on the precise scope of the obligation to prevent. Though *Trail Smelter* is often said to stand for a

---

159. *Id.* art. 2, cmt. ¶ 2.

160. *Id.* art. 2, cmt. ¶ 4.

161. *Id.* In *Trail Smelter*, the tribunal held the threshold to be "serious consequences." Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1938). Similarly, the tribunal in the *Lake Lanoux* award used the concept of *gravement* to emphasize that liability would not lie for *de minimis* harms. Lake Lanoux (Spain v. Fr.), 12 R.I.A.A. 281 (1957). The threshold is likewise recognized in a number of international conventions. *See, e.g.*, Convention on the Regulation of Antarctic Mineral Resource Activities, art. 4, ¶ 2, *opened for signature* June 2, 1988, 27 I.L.M. 859 (not yet in force); Convention on Environmental Impact Assessment in a Transboundary Context, art. 2, ¶¶ 1–2, *opened for signature* Feb. 25, 1991, 1989 U.N.T.S. 309 (entered into force Sept. 10, 1997); Convention on the Law of the Non-navigational Uses of International Watercourses, art. 7, *opened for signature* May 21, 1997, 36 I.L.M. 700 (not yet in force).

162. Draft Articles on Transboundary Harm, *supra* note 146, art. 2, cmt. ¶ 4.

163. *Id.* art. 1, cmt. ¶ 16.

164. *Id.*

165. *Id.* cmt. ¶ 17.

principle of strict liability,[166] the scope of the obligation to prevent transboundary harm is one of due diligence.[167] In order to understand the contours of this obligation, this section surveys the approaches taken to the due diligence concept by arbitral tribunals, the ICJ and the ILC in the *Draft Articles on Transboundary Harm.*

In the *Alabama* claims arbitration,[168] the tribunal examined the proposed definitions of due diligence submitted by the United States and the United Kingdom. Among other things, the case dealt with an American claim that Britain had violated neutrality by permitting the construction of the *CSS Alabama* on its territory with the knowledge that it would be used by the Confederate States Navy.[169] The United States alleged that the United Kingdom did not fulfill an obligation of due diligence to prevent its territory from being used for purposes that breached the law of neutrality.[170]

In argument, the two states offered differing accounts as to the scope of the due diligence obligation. The United States proposed that due diligence was proportional to the "magnitude of the subject and to the dignity and strength of the power which is to exercise it."[171] In this respect, due diligence required the use of "active vigilance" to "prevent its soil from being violated" and to "deter designing men from committing acts of war upon the soil of the neutral against its will."[172] The United Kingdom, for its part, responded with a considerably lower threshold, defining due diligence as "such care as Governments ordinarily employ in their domestic concerns."[173] The tribunal was not persuaded by the British approach, noting with concern that the British definition would "narrow the international duties of a Government to the exercise of the restraining

166. *See, e.g.*, J.G. LAMMERS, POLLUTION OF INTERNATIONAL WATERCOURSES: A SEARCH FOR SUBSTANTIVE RULES AND PRINCIPLES OF LAW 524 (1984).

167. Draft Articles on Transboundary Harm, *supra* note 146, art. 3, cmt. ¶¶ 7–11.

168. The *Alabama Claims* arbitration concerned Britain's breach of neutrality, but its application of due diligence is applicable in the transboundary claims context as well. *See* Draft Articles on Transboundary Harm, *supra* note 146, art. 3, cmt. ¶ 9. For an excellent overview of the arbitral decision and its history, see Tom Bingham, *The* Alabama *Claims Arbitration*, 54 INT'L & COMP. L.Q. 1 (2005).

169. *The Geneva Arbitration (Alabama Claims)*, *in* 1 J.B. MOORE, HISTORY AND DIGEST OF THE ARBITRATIONS TO WHICH THE UNITED STATES HAS BEEN A PARTY 495 (1898).

170. The parties differed to a considerable degree on the appropriate substantive law of neutrality. *See* Bingham, *supra* note 168, at 3.

171. Alabama Claims, *supra* note 169, at 572–73.

172. *Id.* at 573.

173. *Id.* at 612.

powers conferred upon it by municipal law."[174] Thus, in the view of the tribunal, due diligence could not be circumscribed by a nation's own municipal law. Rather, if the existing municipal laws were "insufficient" to permit a state to fulfill its international obligations, then the state should be correspondingly obligated to amend those laws to maintain compliance.[175]

In *United States Diplomatic and Consular Staff in Tehran*, the ICJ addressed in more detail a state's obligation of due diligence with respect to harm to foreign nationals by activities of non-state actors.[176] That case dealt with the seizure of the United States Embassy in Tehran by an armed crowd, instigated by the U.S. grant of asylum to the deposed Shah shortly after the 1979 Iranian Revolution. Though the case principally concerns diplomatic immunity,[177] the issue of state responsibility was essential to the Court's holding that Iran was liable. There was no indication that the armed group was associated with Iranian authorities.[178] However, the Court noted that Iranian forces "are reported to have simply disappeared from the scene" and that there was "no apparent effort to deter or prevent the demonstrators from seizing the Embassy's premises."[179] Thus, the Court concluded that though the acts by the protestors could not be directly attributed to Iran, the State was nonetheless internationally responsible because of its acts or omissions with respect to the seizure.[180]

Though this responsibility entailed a breach of Iran's treaty obligations,[181] the Court nonetheless also found that Iran had breached its obligation under general international law to "ensure 'the most constant protection and security' to each other's nationals

---

174. *Id.* at 613.

175. *See id.*

176. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3 (May 24).

177. *See* Bert V. A. Röling, *Aspects of the Case Concerning United States Diplomatic and Consular Staff in Tehran*, 11 NETH. Y.B. INT'L L. 125 (1980).

178. U.S. v. Iran, *supra* note 176, ¶ 17.

179. *Id.* In its analysis, the Court divided the events into "two phases." The first covered the attack on the embassy and the taking of hostages. *Id.* ¶¶ 56–57. The second phase covered "the whole series of facts which occurred following the completion of the occupation of the United States Embassy by the militants, and the seizure of the Consulates at Tabriz and Shiraz." *Id.* ¶ 69.

180. *Id.* ¶ 61.

181. Namely the 1963 Vienna Convention on Consular Relations and the 1961 Vienna Convention on Diplomatic Relations. *Id.* ¶ 67.

in their respective territories,"[182] and in so doing, affirmed an obligation of due diligence with respect to preventing harm to foreign nationals. According to Pierre-Marie Dupuy, had Iran "been willing and able to demonstrate that it had actually taken all appropriate steps to avoid the taking of diplomats as hostages, then it would not have been held responsible by the court."[183] In this respect, Iran had breached an obligation of conduct, rather than an obligation of result.[184] What mattered was Iran's breach of its "best efforts obligation," not the "end result actually achieved."[185]

In the *Draft Articles on Transboundary Harm*, the ILC likewise derived a standard of due diligence.[186] As articulated by the ILC, due diligence requires the "reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures, in a timely fashion, to address them."[187] This sliding scale approach varies the level of due diligence required based on what is "generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance."[188] In this respect,

182. *Id.*

183. Pierre-Marie Dupuy, *Reviewing the Difficulties of Codification: On Ago's Classification of Obligations of Means and Obligations of Result in Relation to State Responsibility*, 10 EUR. J. INT'L L. 371, 379 (1999).

184. *Id. See also* Special Rapporteur on State Responsibility, *Second Report on State Responsibility*, Int'l L. Comm'n, U.N. Doc. A/CN.4/498 (Mar. 17, 1999).

185. Dupuy, *supra* note 183, at 379. This "best efforts" criterion was recognized in the ILC's *Articles on State Responsibility*. In his commentary to the articles, Special Rapporteur James Crawford noted "[o]bligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur." Draft Articles on State Responsibility, *supra* note 152, art. 14, cmt. ¶ 14.

186. Draft Articles on Transboundary Harm, *supra* note 146, art. 3, cmt. ¶¶ 7–8. The ILC derived the principle from general international law, but also specifically with reference to conventions and other agreements between states. For example, in his commentary, the Special Rapporteur points to the United Nations Convention on the Law of the Sea, Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter, the Vienna Convention for the Protection of the Ozone Layer, the Convention on the Regulation of Antarctic Mineral Resource Activities, the Convention on Environmental Impact Assessment in a Transboundary Context, and the Convention on the Protection and Use of Transboundary Watercourses and International Lakes. *See id.* at 392 n.925. Presumably, though the Rapporteur does not say so explicitly, the due diligence principle is considered a principle of customary international law, whether it be bound up in the substantive obligation or not.

187. *Id.* cmt. ¶ 10.

188. *Id.* cmt. ¶ 11.

more hazardous activities may require a higher standard of care than less hazardous activities. Thus, the ILC stated that the standard may be affected by a variety of factors including the "size of the operation; its location, special climate conditions, materials used in the activity."[189] Because all of these factors may be influenced by technological and scientific advances, the flexible standard requires states to appropriately recalibrate their diligence over time.[190] Similarly, the ILC noted that the "economic level" of states may be taken into account into the determination of whether a state has met its duty of due diligence.[191] Finally, the ILC stated that due diligence requires a state to "take all necessary measures to prevent significant transboundary harm or at any event to minimize the risk thereof."[192]

B. The Obligation to Prevent Transboundary Cyberharm

While the international community has begun an effort to foresee ways international law will regulate cyber attacks that rise to the level of "cyberwarfare" and thus implicate the law of armed conflict,[193] as we have seen, this legal regime does not regulate cyber-

189. *Id.*

190. *Id.* ("Hence, due diligence in ensuring safety requires a State to keep abreast of technological changes and scientific developments.").

191. *Id.* cmt. ¶¶ 12–13. The Special Rapporteur noted the language of the Rio Declaration, which stated that "[s]tandards applied by some countries may be inappropriate and of unwarranted economic and social cost to other countries, in particular developing countries." Rio Declaration, *supra* note 132, Principle 11.

192. Draft Articles on Transboundary Harm, *supra* note 146, cmt. ¶ 14. The Special Rapporteur noted that this reflected Principle 15 of the Rio Declaration and would similarly fluctuate depending on the capacity of the state.

193. For example, a leading proposal determines that an effects-based inquiry can be used to determine whether a cyberattack rises to the level of a use of force or an armed attack, implicating the U.N. Charter or customary *jus ad bellum* principles. Schmitt, *Computer Network Attack*, *supra* note 18, at 914–15. Consensus appears to be coalescing around the effects approach. According to Harold Koh, then-Legal Adviser at the U.S. Department of State, "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." Harold Hongju Koh, Legal Adviser of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm. The recent release of the so-called "Tallinn Manual," a proposed set of guidelines for the state of customary international law as to cyberwarfare, echoes this approach, describing a cyber operation as rising to a "use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." TALLINN MANUAL, *supra* note 18, at Rule 11; *see also* Hathaway et al., *supra* note 17. This makes some intuitive sense. It narrows the scope considerably to only the most severe of

harm that does not reach this threshold, but is nonetheless significantly harmful.[194] In this Part, I argue that the principles of transboundary harm may provide the structure for how international law may regulate these forms of cyberharm.[195] First, this Part examines how the notion of cyberspace can be reconciled with the territorial basis for liability for transboundary harm. Second, this Part explores how the other elements of transboundary harm translate to adequately regulate transboundary cyberharm.[196]

1. Territorial Sovereignty, the Internet & Intellectual Property

In some of the earliest days of the Internet, John Perry Barlow, a former lyricist for the Grateful Dead, wrote a "Declaration of

---

cyberattacks, excluding most cyber operations from the ambit of the laws of war.

194. *See supra* Part I.B.

195. Although at first blush it may appear as though the principles of transboundary harm may be limited to environmental harm, it has been extended to other contexts. As Luke Lee explains, at bottom, the duty to prevent transboundary harm is rooted in the "responsibility which derives from the fact of control over territory." Luke T. Lee, *The Right to Compensation: Refugees and Countries of Asylum*, 80 AM. J. INT'L L. 532, 554 n.92 (1986) ("It has been pointed out that 'to compare the flow of refugees with the flow of, for example, noxious fumes may appear invidious; the basic issue, however, is the responsibility which derives from the fact of control over territory.'"); *see also* GUY GOODWIN-GILL, THE REFUGEE IN INTERNATIONAL LAW 228 n.49 (1983) (extending to the context of refugee flows). It may be worth noting that there may be other corollary obligations, for example, the duty to apprehend or punish non-state actors who are responsible for harms against another state. *See, e.g.*, Massey (U.S.) v. Mex., 4 R.I.A.A. 155 (Mex./U.S. Gen. Claims Comm'n 1927); Youmans (U.S.) v. Mex., 4 R.I.A.A. 110 (Mex./U.S. Gen. Claims Comm'n 1926); Janes (U.S.) v. Mex., 4 R.I.A.A. 82 (Mex./U.S. Gen. Claims Comm'n 1925); *see also* IAN BROWNLIE, SYSTEM OF THE LAW OF NATIONS: STATE RESPONSIBILITY PART I 161 (1983) (discussing these cases).

196. Some scholars have analogized cyberharm to espionage. *See, e.g.*, Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162 (2011). And there is ongoing debate whether espionage during peacetime is a breach of an international legal obligation. *Compare* Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 347 (1996) (finding that espionage is not a violation of international law), *with* Manuel R. García-Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. PITT. L. REV. 65, 79–80 (1964) (arguing that peacetime espionage is a violation of international law). *See also* Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67 (1984) ("[E]spionage in peacetime is contrary to international law, even if it does not involve any 'trespass'; espionage appears to be illegal under international law in time of peace if it involves the presence of agents sent clandestinely by a foreign power into the territory of another state. Such operations offend the principle of peaceful cooperation of states.").

Independence" for cyberspace.[197] His grandiose claim typified an optimistic view held by some American academics in the mid-to-late nineties.[198] Because "code is law,"[199] so the argument went, the Internet could be considered "sovereign" in its own right and not beholden to the traditional boundaries of national sovereignty.[200] This viewpoint was emboldened by arguments that the foundation of the Internet made it such that effects by online activities were not geographically specific, but could be felt in a variety of geographical locations at once and depending on context.[201] Vint Cerf, a computer scientist who has been described as one of the "fathers of the Internet,"[202] wrote that "[t]he Internet was designed without any contemplation of national boundaries. The actual traffic in the Net is totally unbound with respect to geography."[203]

---

197. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html (last visited Jan. 28, 2013).

198. It was also the subject of considerable debate. *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998) [hereinafter Goldsmith, *Territorial Sovereignty*]; Steven M. Hanely, *International Internet Regulation: A Multinational Approach*, 16 J. MARSHALL J. COMPUTER & INFO. L. 997 (1998); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (asserting sovereignty for cyberspace); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1407 (1996) (responding to Johnson & Post); Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423 (1998); David G. Post, *The "Unsettled Paradox": The Internet, The State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521 (1998); Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647 (1997).

199. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). Lessig, however, slightly modified his view in light of the developments of the Internet over time. *See* LAWRENCE LESSIG, CODE VERSION 2.0 (2006).

200. *Compare* LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, *supra* note 199, *and* Johnson & Post, *supra* note 198, at 1367 (arguing that "[c]yberspace . . . needs and can create its own law and legal institutions" and that "territorial authorities may yet learn to defer to the self-regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services."), *with* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006).

201. *See* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178–83 (1997); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 917–19 (1996).

202. Gregory Ferenstein, *'Father of the Internet', Vint Cerf, Says Government Gets Credit for Inventing Web*, TECHCRUNCH (July 26, 2012), http://techcrunch.com/2012/07/26/father-of-the-internet-vint-cerf-says-government-gets-credit-for-inventing-web/.

203. Lisa Guernsey, *Welcome to the Web. Passport, Please?*, N.Y. TIMES (Mar. 15,

This view, however, has not exactly taken root.[204] For example, in its official statement on the subject, the Chinese government announced that its view of Internet sovereignty did not mean the Internet was sovereign, but that individuals using the Internet in China would have to follow Chinese law.[205] The implications in China are particularly severe as China is among the leaders in filtering Internet services.[206] Less systematic, but nonetheless considerable, control over Internet content exists elsewhere, including in the United States.[207]

While in the early days geo-location was difficult, end users are ordinarily automatically geo-located through the use of "tracing" packets, which report the path the packet travels.[208] Though there are ways to hide one's source,[209] most users can be geo-located easily at least at the country level. As a result, states regulate the Internet within their own territory by governing the local connections within their borders, including end-users, Internet intermediaries, and hard-

---

2001), http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html.

204. Even some of the fiercest proponents of sovereignty for the Internet have tempered their claims considerably, recognizing the role of territorial sovereigns. *Compare* David R. Johnson et al., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 1 (2004) (acknowledging that "traditional sovereigns can and should play an important role in regulating many actions and actors that affect the Internet."), *with* Johnson & Post, *supra* note 198 (arguing that "[c]yberspace . . . needs and can create its own law and legal institutions" and that "territorial authorities may yet learn to defer to the self-regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services.").

205. *See The Internet in China*, PEOPLE'S DAILY ONLINE (June 8, 2010), http://english.peopledaily.com.cn/90001/90776/90785/7017177.html; *see also* Evan Osnos, *Can China Maintain "Sovereignty" over the Internet?*, THE NEW YORKER (June 11, 2010), http://www.newyorker.com/online/blogs/evanosnos/2010/06/what-is-internet-sovereignty-in-china.html.

206. *See* Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L L. 263, 265 (2006).

207. For example, at the insistence of the New York State Attorney General, Verizon dropped Usenet newsgroups deemed to be in furtherance of violations of New York law. Danny Hakim, *Net Providers to Block Sites with Child Sex*, N.Y. TIMES, June 10, 2008, http://www.nytimes.com/2008/06/10/nyregion/10internet.html; *see also* Declan McCullagh, *N.Y. Attorney General Forces ISPs to Curb Usenet Access*, CNET NEWS (June 10, 2008, 12:09 PM), http://news.cnet.com/8301-13578_3-9964895-38.html.

208. *See* GOLDSMITH & WU, *supra* note 200, at 60.

209. *See* NRC Report, *supra* note 18, at 100. One of the most common ways to hide one's location is the use of "proxy servers." *See Geolocation: Don't Fence Web In*, WIRED (July 12, 2004), http://www.wired.com/techbiz/it/news/2004/07/64178?currentPage=all.

ware.[210] These local intermediaries, or the "people, equipment, and services within national borders that enable local Internet users to consume" the Internet services,[211] provide government with the ability to control end users by regulating access.[212] Moreover, on the back-end, most Internet usage has effects in the real world, providing the basis for prescriptive and adjudicatory jurisdiction.[213]

With sovereign control comes the basis for sovereign prerogative and sovereign obligation. Though the absolute nature of territorial sovereignty is perhaps a frail notion,[214] these principles of sovereignty still undergird much of international law.[215] While some might find China's filtering processes undesirable for any number of reasons,[216] a state's right to regulate activities within its territory allow that nation to regulate the "local effects of extraterritorial acts,"[217] and the success of much of online commerce depends, in part, on the protection and enforcement of property and contract

---

210. *See* Goldsmith, *Territorial Sovereignty*, *supra* note 198, at 481; *see also* Goldsmith, *Against Cyberanarchy*, *supra* note 198.

211. *See* GOLDSMITH & WU, *supra* note 200, at 68.

212. *Id.*

213. *See* Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1197 (1999); *cf.* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 402(1)(c), 403, 421(j) (1987) (stating that "substantial" effect is a basis for jurisdiction).

214. STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 4 (1999) (separating out four defined concepts of sovereignty: legal, interdependence, domestic, and Westphalian (territorial)). In some respects, European integration may be some of the most concrete evidence of states giving up portions of their sovereign prerogatives. The creation of the European Union, for example, disentitles European states from using traditional sovereign powers *vis-à-vis* other member states. Notably, the permissibility of countermeasures is severely restricted. *See, e.g.*, Joined Cases 90/63 and 91/63, Comm'n v. Lux. & Belg., 1964 E.C.R. 625, 631; Case 232/78, Comm'n v. Fr., 1979 E.C.R. 2730, 2739; Case 52/75, Comm'n v. It, 1976 E.C.R. 278, 284.

215. For example, sovereignty is perhaps the centerpiece of the U.N. Charter. *See, e.g.*, U.N. Charter art. 2 para. 1 (reaffirming "the principle of the sovereign equality of all its Members"). This is not to say it has persisted without significant protest. Louis Henkin, for example, once wrote that sovereignty was a "bad word, not only because it has served terrible national mythologies; in international relations, and even in international law, it is often a catchword, a substitute for thinking and precision." LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 8 (1995). For what it's worth, I hope to avoid Professor Henkin's admonition.

216. *See* GOLDSMITH & WU, *supra* note 200, at 87–98 (describing China's filtering system to block or censor websites).

217. Goldsmith, *Territorial Sovereignty*, *supra* note 198, at 476. *But see* Larry Kramer, *Vestiges of Beale: Extraterritorial Application of American Law*, 1991 SUP. CT. REV. 179, 202 (1991).

rights.[218] Conversely, territorial sovereignty may entail a state's responsibility for regulating the acts of individuals inside its own territory using the Internet.[219]

2. Translating the Due Diligence Obligation to Transboundary Cyberharm

Given the continuing relevance of territorial sovereignty in the regulation of the Internet, an adequate international legal regime for transboundary cyberharm must take cognizance of territorial sovereignty's prerogatives and its obligations. What the tradition of transboundary harm teaches us is that territorial sovereignty entitles a state to protection from significant harm to sovereign rights while obliging states to exercise due diligence in ensuring their own territory is not used to cause such harm.

It is tempting to misuse analogies. There is something alluring about the idea of analogizing individual IP packets of information to particulate matter.[220] But the vast majority of packets of information are not pollutants or harmful byproducts of otherwise beneficial production. Even those packets that are malicious vary in scope, complexity, and purpose. The harm caused by DDoS attacks, for example, is not the harm to a computer system, but the prevention of access to that system for genuine end-users.[221] In contrast, the harm caused by most APTs may not be realized until years after the loss of confidential information.[222]

More difficult still is assigning value to losses incurred as a result of APT-related theft.[223] It is indisputable that Coca-Cola suffered harm when its $2.4 billion deal to purchase China Huiyan Juice

---

218. *See* GOLDSMITH & WU, *supra* note 200, at 140 ("[t]he success of Internet companies like eBay, the success of the Internet itself, and indeed the success of many human endeavors depend on something invisible but essential: public goods like criminal law, property rights, and contract enforcement provided by government.").

219. *See* Goldsmith, *Territorial Sovereignty*, *supra* note 198, at 476.

220. *See supra* notes 31–38 and accompanying text.

221. *See supra* Part I.B.1.

222. *See* ONCIX Report, *supra* note 124, at 3 (noting that "[m]any victims of economic espionage are unaware of the crime until years after loss of the information.").

223. *See id.* (stating that "it is inherently difficult to assign an economic value to some types of information that are subject to theft. It would, for example, be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a U.S. company and foreign counterparts.").

Group was sunk by an APT originating in China.[224] But assigning a value to that loss is irreducibly speculative. Should we assess Coca-Cola's loss by the value of the deal or its lost profits? At the other extreme, should we limit the loss merely based on Coca-Cola's cost for increased security?

It would be an error, however, to mistake the presence of speculation for the need for certainty. As I argue later in this Note, in part because of the speculative nature of the harm, remedies such as trade sanctions or financial liability will frequently be imprecise and ineffective tools as reciprocal measures.[225] But while these assessments are important in determining liability for private actors as a matter of municipal law, they are less applicable in the context of the international law of transboundary cyberharm.[226] To see why, recall that the principles of transboundary harm distinguish between liability and state responsibility.[227] The logic behind this distinction is that because the relevant acts themselves are not violations of international law—for example, mining a territorial sea in *Corfu Channel*,[228] or polluting the air in *Trail Smelter*—the question of state responsibility for those acts is irrelevant. The breach is the failure to exercise due diligence in preventing those acts from causing significant harm to another state.[229] At bottom, the duty is to exercise the prerogatives of

224. *See* Elgin et al., *supra* note 89 (on the Coca-Cola APT that resulted in the loss of a major acquisition).

225. *See infra* Part III.B.

226. One quirk of the *Trail Smelter* award, it is worth noting, is that the arbitral tribunal held Canada liable for damages. Whatever the merit of that decision, it does not affect my reasoning here.

227. *See, e.g.*, Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 18 (Apr. 9); Draft Articles on Transboundary Harm, *supra* note 146, art. 1, ¶ 6.

228. Recall that in *Corfu Channel*, the breach was not the mining of the sea, but Albania's failure to notify Britain. *See* 1949 I.C.J. at 186.

229. For example, in *Trail Smelter*, the ultimate dispute concerned finding a balance between Canada's ability to smelt lead and zinc on its territory, and the U.S. right to determine how best to use its territory, in that case to grow apples undamaged by smelter pollution. *See* Austen L. Parrish, *Sovereignty's Continuing Importance: Traces of* Trail Smelter *in the International Law Governing Hazardous Waste Transport*, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION, 181, 183, (Rebecca M. Bratspies & Russell A. Miller eds., 2006). In this way, the arbitral tribunal's decision was not focused on environmental harm *per se*, but was firmly rooted in principles of noninterference in state sovereignty. Similarly, *Corfu Channel*, though concerning activities inside Albanian territorial waters, did not hold that the placement of mines inside one's territory was *per se* a violation of international law. Instead, the ICJ held that Albania's knowledge of the mines, and its failure to warn other states, violated its obligation to prevent its "territory" from being used "contrary to the

territorial sovereignty with respect to another state's sovereignty.[230]

III. A DECENTRALIZED SOLUTION FOR A DECENTRALIZED SYSTEM

Due in part to the sovereign equality of nations,[231] the international legal system has no supranational government. As Louis Henkin wrote, there is no "executive authority with power to enforce the law. There is no police system whose pervasive presence might deter

---

rights of other States." *Corfu Channel*, 1949 I.C.J. at 20–22. A related principle is the nebulous notion of nonintervention. In the most abstract sense, the principle is said to prohibit a state from intervening in the internal affairs of another sovereign state. *See, e.g.*, Convention on Rights and Duties of States art. 8, Dec. 26, 1933, 49 Stat. 3097, 165 L.N.T.S 19 ("No state has the right to intervene in the internal or external affairs of another."); Charter of the Organization of American States art. 19, Apr. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3 ("No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements."); U.N. Charter art. 2, para. 7 (stating that states shall be free from intervention by the U.N. "in matters which are essentially within the domestic jurisdiction of any state."). *See also* Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs*, 83 AM. J. INT'L L. 1, 7 (1989). Most of the scholarly literature has focused on "forcible influence," and the dividing line between appropriate intervention and impermissible intervention is murky at best.

230. The law of neutrality in armed conflict provides another illustration of this principle. The international law of neutrality regulates the behavior of states not currently in an armed conflict, imposing an obligation of non-participation and impartiality with respect to warring states. *See* Michael Bothe, *The Law of Neutrality*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 485, 486 (Dieter Fleck ed., 1995) ("The duty of non-participation means, above all, that the state must abstain from supporting a party to the conflict," which includes a defense of that neutrality against others who may seek to use the state's resources. "The duty of impartiality . . . means that the neutral state must apply the specific measures it takes on the basis of the rights and duties deriving from its neutral status in a substantially equal way as between the parties to the conflict . . . ."). These principles are enshrined in the Hague Conventions of 1907, which, for example, prohibit a state from allowing troops or supplies to move across the territory of a neutral state, the formation of belligerent combatants on neutral territory, or providing military supplies to one of the belligerent states. Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land arts. 2, 4–5, 10, Oct. 18, 1907, 36 Stat. 2310. If these prohibitions are in some way violated, the offended state is expressly permitted to demand reparation or take other measures to "exact the necessary reparation." L.F.L. OPPENHEIM, INTERNATIONAL LAW 753 (7th ed. 1952) ("Violations of neutrality . . . may at once be repulsed, and the offended party may require the offender to make reparation, and, if this is refused, may take such measures as he thinks adequate to exact the necessary reparation.").

231. *See supra* Part II.B.1.

violation."[232] As a result, enforcement is not "systematic or centrally directed, and . . . accordingly [sanctions] are precarious in their operation."[233] In this respect, the international system is not so dissimilar from the Internet. Both realms feature a lack of centralized control—the primary vehicle of enforcement in international law is the "untrammeled right to self-help."[234]

In this Part, I argue that this decentralized enforcement apparatus applies just the same in the context of transboundary cyberharm. When a state fails to prevent transboundary cyberharm, its breach of that obligation entitles offended states to respond through the use of proportionate countermeasures—that is, they are entitled to *neglect* their own obligation to prevent. First, this Part provides an overview of decentralized enforcement in international law—that it is, in large part, a feature and not a bug.[235] In particular, this Part details the mechanism of proportionate countermeasures and then shows how that doctrine applies in the context of transboundary cyberharm.

---

232. LOUIS HENKIN, HOW NATIONS BEHAVE 24 (2d ed. 1979).

233. J.L. BRIERLY, THE LAW OF NATIONS: AN INTRODUCTION TO THE INTERNATIONAL LAW OF PEACE 101 (6th ed. 1963).

234. Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 1, 18 (Stephen D. Krasner ed., 1983); *see also* DAVID J. BEDERMAN, THE SPIRIT OF INTERNATIONAL LAW 187–94 (2002). This is not to suggest, however, that unilateral self-help is the *only* way international law constrains states. Indeed, it is perhaps a truism that "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time." HENKIN, *supra* note 232, at 47 (emphasis omitted). Harold Koh has explained international legal compliance in almost Hartian terms, referring to its internalization among transnational actors. *See generally* Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599 (1997). Institutionalists have found ways to root compliance in traditional game theory. *See, e.g.*, ROBERT O. KEOHANE, AFTER HEGEMONY (1984); Robert O. Keohane & Lisa L. Martin, *The Promise of Institutionalist Theory*, 20 INT'L SECURITY 39, 41–42 (1995); JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 27–28 (2005). By contrast, Thomas Franck viewed international law as exerting constraint if it emerged through legitimate processes and thus pulling toward compliance. *See* THOMAS M. FRANCK, THE POWER OF LEGITIMACY AMONG NATIONS 24 (1990). Constructivists argue from somewhat of a different angle, such that state interests are a function of an international legal system. *See, e.g.*, JOHN GERARD RUGGIE, CONSTRUCTING THE WORLD POLITY (1998); ALEXANDER WENDT, SOCIAL THEORY OF INTERNATIONAL POLITICS (1999). This Note, in short, does not take a position on any of these views. That would be far out of its scope. It is merely sufficient to note that unilateral enforcement is consistent with, and recognized by, nearly all of these theories of international relations and international law.

235. *See* Oona Hathaway & Scott J. Shapiro, *Outcasting: Enforcement in Domestic and International Law*, 121 YALE L.J. 252, 300–20 (2011); *see also* Draft Articles on State Responsibility, *supra* note 152, arts. 51, 53.

A. Decentralized Enforcement in International Law

The principle of reciprocity—that is, returning like behavior with like—is a central feature of international law,[236] a system with no external enforcement authority other than its own members.[237] In the context of the use of force, this notion is perhaps enshrined by Article 51 of the U.N. Charter, recognizing the "inherent right of . . . self-defense" following an armed attack.[238]

But this right of self-defense is strictly circumscribed to cases of an "armed attack."[239] For harms that do not meet the threshold for armed attacks, states may use "retorsions" and "reprisals," or

---

236. International law is not alone in relying on reciprocal enforcement mechanisms. In domestic legal systems, self-help has long been recognized to protect the person in cases of self-defense or the protection of property. *See, e.g.*, Kimberly Kessler Ferzan, *Self-defense and the State*, 5 OHIO ST. J. CRIM. L. 449 (2008); Kenneth W. Simons, *Self-Defense: Reasonable Beliefs or Reasonable Self Control?*, 11 NEW CRIM. L. REV. 51 (2008); RESTATEMENT (SECOND) OF TORTS §§ 63, 77 (1965); MODEL PENAL CODE, §§ 3.04, 3.06 (1985).

237. There are, of course, some exceptions to this reciprocity regime. Among others, for example, authorization for the use of military force by the United Nations Security Council. *See* U.N. Charter arts. 39–51; S.C. Res. 1973, U.N. Doc. S/RES/1973 (Mar. 17, 2011) (authorizing the use of force in Libya). Additionally, some international legal regimes specifically do not contemplate reciprocity. For example, the *jus in bello* obligations of the law of armed conflict do not depend on reciprocity, but rather apply "in all circumstances." *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 1, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, art. 1, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War art. 1, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 1, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

238. U.N. Charter art. 51. This right has perhaps extended to the use of self-defense against non-state actors, especially if that state is "unwilling or unable" to prevent the continuing threat. *See generally* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012) (explaining that though there are disputes as to the elements of the "unwilling or unable" test, it is recognized as an accepted principle of international law).

239. One of the best-known models for determining whether a use of cyberforce rises to the level of an "armed attack" for the purposes of Article 51 is the "effects" based model offered by Michael Schmitt. *See* Schmitt, *Normative Framework*, *supra* note 18, at 914–15. Schmitt's model considers the severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy of a cyberattack in order to determine whether it meets the threshold. *Id.* For other accounts of when cyberattacks might rise to the level of "armed attack," see, e.g., Hathaway et al., *supra* note 17; Graham, *supra* note 18, at 90–92; Sklerov, *supra* note 16; Jensen, *supra* note 16; Kesan & Hayes, *supra* note 16.

proportionate countermeasures, in response to an attack or harm.[240] Retorsions are considered "unfriendly but nevertheless lawful act[s] by the aggrieved party against the wrongdoer"[241] and are relatively unregulated by international law.[242] Reprisals, however, are acts "otherwise illegal, performed by a state for the purpose of obtaining justice for an international delinquency by taking the law into its own hands."[243]

These "countermeasures," taken in response to wrongful conduct by another state, are seen as lawful methods to enforce compliance in a necessarily decentralized system. James Crawford, Special Rapporteur for State Responsibility for the International Law Commission (ILC), underlined this point, "[c]ountermeasures are a feature of a decentralized system by which injured States may seek to vindicate their rights . . . ."[244]

---

240. *See, e.g.*, Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 127 (June 27); Gabcikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 55–56 (Feb. 5); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 905 (1987) (" . . . a state victim of a violation of an international obligation by another state may resort to countermeasures that might otherwise be unlawful . . . ."); Draft Articles on State Responsibility, *supra* note 152, arts. 22, 51, 53 ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State . . . .").

241. ELIZABETH ZOLLER, PEACETIME UNILATERAL REMEDIES: AN ANALYSIS OF COUNTERMEASURES 5 (1984).

242. *But see* John K. Setear, *Responses to Breach of a Treaty and Rationalist International Relations Theory: The Rules of Release and Remediation in the Law of Treaties and the Law of State Responsibility*, 83 VA. L. REV. 1, 75–76 (1997) (arguing that retorsions should be subject to the limits of necessity and proportionality).

243. L.F.L. OPPENHEIM, INTERNATIONAL LAW 136 (7th ed.).

244. Draft Articles on State Responsibility, *supra* note 152, arts. 51, 53. In their article on "outcasting" in domestic and international law, Oona Hathaway and Scott Shapiro identified countermeasures as a form of "simple outcasting" and an essential feature of international law by which states enforce international law. *See generally,* Hathaway & Shapiro, *supra* note 235. This form of enforcement is "external" because the legal regime itself does not impose sanctions, but instead relies on the states for enforcement. *Id.* at 307; *see also* Anthony D'Amato, *Is International Law Really "Law"?*, 79 NW. U. L. REV. 1293, 1303, 1310–13 (1984) (describing this phenomenon as "reciprocal entitlement" violations). Outcasting differs from traditional domestic legal enforcement measures in that it frequently does not require the use of physical force, instead relying on members of a given society withdrawing benefits from the outcast. *See* Hathaway & Shapiro, *supra* note 235. For example, in the European Union, the principles of direct effect and European Community law supremacy provide a basis for private individuals to sue national governments for non-compliance. Jonas Tallberg, *Paths to Compliance: Enforcement, Management, and the European Union*, 56 INT'L ORG. 609, 621 (2002). Similarly, in disputes before the World

B. Proportionate Countermeasures: Magnitude and Form

In its Articles on the Responsibility of States for Internationally Wrongful Acts, an effort that took more than half a century to conclude with the help of five special rapporteurs,[245] the ILC defined countermeasures as "measures, which would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State" if "they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[246] The Draft Articles places significant constraints on the use of countermeasures, acceptable only when a prior wrongful act may be attributed to the aggressor state,[247] thereby likely excluding countermeasures taken in response to acts by non-state actors.[248] The ILC's elements for lawful countermeasures relies

---

Trade Organization (WTO), the Agreement on Subsides and Countervailing Measures not only expressly permits countermeasures if authorized by the WTO Dispute Settlement Body (DSB), it explicitly contemplates them as the primary enforcement mechanism. Agreement on Subsidies and Countervailing Measures, arts. 7.9, 7.10, WTO Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1869 U.N.T.S. 14 (1999). In this sense, "[t]he WTO has no jailhouse, no bail bondsmen, no blue helmets, no truncheons or tear gas." Hathaway & Shapiro, *supra* note 35 (quoting Hippler Bello at 267). Nonetheless, it is able to enforce its rule by relying on victim states to respond through authorized trade sanctions. *See, e.g.*, Decision by the Arbitrators, Brazil-Export Financing Programme for Aircraft, Recourse to Arbitration by Brazil Under Article 4.11 of the SCM Agreement, WT/DS46/ARB (adopted Aug. 28, 2000).

245. Daniel Bodansky, John R. Crook & David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817 (2002).

246. Rep. of the Int'l Law Comm'n, 53rd sess., Apr. 23–June 1, July 2–Aug. 10, 2001, at 128, U.N. Doc. A/56/10. GAOR, 56th Sess. Supp. No. 10.

247. Draft Articles on Transboundary Harm, *supra* note 146, art. 49(1).

248. The debate over the right of self-defense against non-state actors is heated. Though this debate was ongoing even before the attacks against the World Trade Center on September 11, 2001, "those events sharpened its focus and gave it greater operational urgency." Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 770 (2012). Some scholars have argued that the language of Article 51 only includes armed attacks by states, and thus does not provide or recognize an inherent right of self-defense against non-state actors. *See, e.g.*, Antonio Cassese, *The International Community's 'Legal' Response to Terrorism*, 38 INT'L & COMP. L.Q. 589, 596 (1989); Eric Myjer & Nigel White, *The Twin Towers Attack: An Unlimited Right to Self-Defense*, 7 J. CONFLICT & SECURITY L. 5, 7 (2002). Others try to allow for self-defense against non-state actors by way of attributing that conduct to a state. This has been the apparent approach of the ICJ. *See, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 194 (holding that Israel could not claim self-defense because it could not attribute any of the alleged armed attacks to a State). *But see* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 (Dec. 19). Others are more open to the idea of

heavily on the ICJ's opinion in the *Gabčíkovo-Nagymaros Project* case.[249] First, countermeasures must only be taken after advance notice and an offer for negotiation,[250] though this provision is subject to an escape valve for "urgent countermeasures" if "necessary to preserve [a state's] rights."[251] Second, they must also be directed solely at the state responsible for the prior wrongful act,[252] used in order to induce compliance,[253] and terminated as soon as the state begins to comply.[254] Additionally, countermeasures cannot violate *jus cogens* norms, or, at least according to the ILC, involve the use of force.[255]

Finally, the countermeasures must be "commensurate" with the wrongful act.[256] The ILC thus inverted the negative formulation used in the *Air Services* case, that countermeasures cannot be "clearly disproportionate."[257] According to the commentary, the negative formulation[258] could have allowed "too much latitude, in a context

---

allowing a right of self-defense against non-state actors, whether it may be attributed to a state or not. *See, e.g.*, Theresa Reinold, *State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11*, 105 AM. J. INT'L L. 244 (2011); Thomas M. Franck, *Terrorism and the Right of Self-Defense*, 95 AM. J. INT'L L. 839, 840 (2001); Christopher Greenwood, *International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq*, 4 SAN DIEGO INT'L L.J. 7 (2003); Michael Byers, *Terrorism, the Use of Force and International Law after 11 September*, 51 INT'L & COMP. L.Q. 401 (2002); Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHI. J. INT'L L. 83 (2003); Jordan J. Paust, *Use of Armed Force Against Terrorists in Afghanistan, Iraq and Beyond*, 35 CORNELL INT'L L.J. 533 (2001); Greg Tracalio & John Altenburg, *Terrorism, State Responsibility and the Use of Military Force*, 4 CH. J. INT'L L. 97 (2003); *see also* Deeks, *supra* note 238 (on the right to self-defense when states are "unwilling or unable" to suppress a threat from inside their territory).

249. *See* Gabčikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7 (Feb. 5).

250. Draft Articles on Transboundary Harm, *supra* note 146, art. 52(1).

251. *Id.* art. 52(2).

252. *Id.* art. 49(1)–(2).

253. *Id.* art. 49(1).

254. *Id.* art. 53.

255. *Id.* art. 50(1). *But see* Separate Opinion of Judge Simma, Oil Platforms (Iran v. U.S.) 2003 I.C.J. 161, 324, 332 (Nov. 6); *see infra* notes 270–72 and accompanying text.

256. *Id.* art. 51.

257. *See infra* notes 261–62 and accompanying text.

258. The ILC's positive formulation of the proportionality test was an apparent departure not only from earlier cases, but also from the prior special rapporteur for state responsibility. *See* Roberto Ago, Special Rapporteur, Third Report on State Responsibility, 2 Y.B. INT'L L. COMM'N, pt. 1, at 69, U.N. Doc. A/CN.4/SER.A/1971/Add.1; *see also* Nicaragua. 1986 ICJ 14 at 368 (dissenting opinion of Judge Schwebel) (citing Ago's Third Report) ("There must of course be some proportion between the wrongful infringement by one State of the right of another State and the infringement by the latter of a right of the

where there is concern as to the possible abuse of countermeasures."[259] It is evident from these restrictions that the ILC was nervous about having too lax standards for countermeasures.[260] As James Crawford, the articles' final special rapporteur, noted in his commentary, "Concerns [about countermeasures] were expressed at various levels. The most fundamental related to the very principle of including countermeasures in the text, either at all or in the context of the implementation of state responsibility."[261] But, according to some scholars, "the primary thrust of these provisions is to superimpose procedural values of rectitude and transparency on states' assessments of countermeasure options, even while incorporating some ambiguities that may constrain such behavior." The result is that, "[i]ronically, the overall effect on the international legal process of the Commission's approach may be to permit more aggressive forms of countermeasures."[262]

C. Countermeasures for Transboundary Cyberharm

As we have seen, reciprocal enforcement is, in part, a function of the decentralization of the international legal system.[263] We have also seen that the Internet is a decentralized system,[264] but that despite this decentralization each nation can exercise considerable control over Internet actors through regulation of end-users.[265] It's clear that the United States feels entitled to countermeasures.[266] The

---

former through reprisals. In the case of conduct adopted for punitive purposes, of specifically retributive action taken against the perpetrator of a particular wrong, it is self-evident that the punitive action and the wrong should be commensurate with each other. But in the case of action taken for the specific purpose of halting and repelling an armed attack, this does not mean that the action should be more or less commensurate with the attack. Its lawfulness cannot be measured except by its capacity for achieving the desired result.").

259. Draft Articles on State Responsibility, *supra* note 152, art. 51, cmt. ¶ 5.

260. *Id.* pt. 3, ch. 2, cmt ¶ 2 ("Like other forms of self-help, countermeasures are liable to abuse and this potential is exacerbated by the factual inequalities between States. [The Draft Articles] has as its aim to establish an operational system, taking into account the exceptional character of countermeasures as a response to internationally wrongful conduct. At the same time, it seeks to ensure, by appropriate conditions and limitations, that countermeasures are kept within generally acceptable bounds.").

261. *Id.* at 48.

262. Bodansky, Crook & Bederman, *supra* note 245, at 819.

263. *See supra* Part III.A–B.

264. *See supra* Part I.A.

265. *See supra* Part II.B.1.

question, then, is the *form* and the *magnitude* that those measures could take.[267]

Before we address that question, however, it's important to recall the notice requirement for countermeasures.[268] This element

---

266. On February 20, 2013, a day after the Mandiant Report on Chinese hacking became public, the White House released a brief (and perhaps hastily written) report entitled the *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, WHITE HOUSE, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (Feb. 2013). The report is a scant twelve pages, with the rest an annex composed mostly of previously published material. *See* Jack Goldsmith, *The USG Strategy to Confront Chinese Cyber Exploitation, and the Chinese Perspective*, LAWFARE (Feb. 21, 2013, 1:17 PM), http://www.lawfareblog.com/2013/02/the-usg-strategy-to-confront-chinese-cyber-exploitation-and-the-chinese-perspective/ [hereinafter Goldsmith, *Chinese Perspective*]. Perhaps the most (if the only) aggressive option was the hint of possible trade sanctions as retribution. *See* Scott Murdoch, *US plans response to China's Hacking*, THE AUSTRALIAN (Feb. 21, 2013), http://www.theaustralian.com.au/news/world/us-plans-response-to-chinas-hacking/story-e6frg6so-1226582185654# ("The Obama administration is reportedly drawing up a retaliatory response to the hacking that is likely to threaten trade sanctions or fines."). In addition to trade sanctions, there are other ways in which a state could respond. The United States could respond with a cyber attack of its own, for example, through USCYBERCOM. The resources and capacity of USCYBERCOM are notoriously kept secret. *See* David Pozen, *The Leaky Leviathan: Why the Government Criminalizes, and Condones, Unauthorized Disclosures of Information*, 127 HARV. L. REV. at 82 n.454 (forthcoming December 2013) (quoting DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 265 (2012) ("Reluctant as the White House is to discuss drones . . . it is absolutely allergic to talking about our cyber-offense capabilities.")). But the Stuxnet event alone shows the breadth of the capacity of the U.S. government in cyberwarfare. *See supra* notes 82–83 and accompanying text. It remains to be seen whether the USG will actually pursue any of the options it outlines in the report—and there are skeptics. *See, e.g.*, Goldsmith, *Chinese Perspective* ("Law enforcement and educational tools are useless as a response to hackers residing in China. And unless the diplomatic and trade law tools are ratcheted up to near-trade-war levels—which the Strategy does not propose, and which I seriously doubt will happen—they are almost certain not to have much of an impact on the problem of Chinese cyber exploitation, especially if, as the USG maintains, the Chinese are reaping such huge rewards from cyber theft.").

267. A state could respond, for example, through trade sanctions. But at the outset, it is questionable whether trade sanctions could ever be sufficient to disincentivize a state such as China from engaging in APTs that bring great benefit to the state. *See* Goldsmith, *Chinese Perspective*, *supra* note 266 (questioning the extent to which trade sanctions would sufficiently deter China from cyber espionage). Additionally, even if such a claim were substantively legitimate, the United States would bear the burden of proving that China was responsible for the underlying cyber espionage. *See* James Headen Pfitzer & Sheila Sabune, *Burden of Proof in WTO Dispute Settlement: Contemplating Preponderance of the Evidence*, ICTSD DISPUTE SETTLEMENT & LEGAL ASPECTS OF INTERNATIONAL TRADE, Issue Paper No. 9 at 22 (April 2009).

268. *See, e.g.*, Draft Articles on State Responsibility, *supra* note 152, art. 52 (noting that a state must make a prior demand that the offending state stop its offending conduct, as

can be met in two ways. First, for states systemically violating their obligation to prevent transboundary harm, this notice has likely already been given. For example, with respect to China, the United States has arguably already issued that notice.[269] Because the violations of international law are not the individual attacks themselves, but rather a state's failure to exercise due diligence to prevent such harm, once notice has been made, ongoing behavior by offending states will justify continued countermeasures. Second, the nature of cyber attacks is that rapid response will often be essential. In these cases, countermeasures may be justified under the customary exception for urgency.[270]

As much as a state may be well equipped to engage in one-off cyber attacks in response to transboundary attacks,[271] the sheer scope of transboundary cyberharm makes responses by the government simply unrealistic.[272] In contrast to the state, however, private actors are better positioned to respond to cyberharm. First, firms can best determine the costs and benefits of retaliatory measures. Firms will

---

well as offer to negotiate).

269. Press Release, U.S. Department of State, Statement on Google Operations in China (Jan. 12, 2010), http://www.state.gov/secretary/rm/2010/01/135105.htm ("We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. [Secretary of State Clinton] will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear.").

270. *See* Draft Articles on State Responsibility, *supra* note 152, art. 52(2) ("Notwithstanding paragraph 1(b) [on notice], the injured state may take such urgent countermeasures as are necessary to preserve its rights."); *see also* Hinkle, *supra* note 17, at 18 (arguing that when applying article 52(2) to the context of cyberattacks, "the nature of cyber-force weighs in favor of an injured state resorting rapidly, and with broad discretion, to countermeasures.").

271. *See supra* notes 82–83 and accompanying text.

272. *See supra* notes 55–59 on statistics of number of attacks; Stewart Baker, *Rethinking Cybersecurity, Retribution, and the Role of the Private Sectors*, SKATING ON STILTS (Sept. 18, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/09/rethinking-cybersecurity-the-role-of-retribution-and-of-the-private-sector.html (estimating that for many companies, fighting ongoing attacks costs up to $50,000–100,000 per week); *see also* Nicole Perlroth, David E. Sanger & Michael S. Schmidt, *As Hacking Against U.S. Rises, Experts Try to Pin Down Motive*, N.Y. TIMES (Mar. 3, 2013), http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html (quoting cybersecurity experts who stated that calls to authorize the military to defend private corporate networks are unrealistic, as "[t]he military has neither the specialized expertise nor the capacity to do this; it needs to address only the most urgent threats.").

hackback if they find that alternative solutions, such as judicial remedies, are ineffective,[273] and if the costs of hacking back[274] are less than the benefits achieved through deterrence and successful disruption.[275] Because in the United States the vast majority of these threats are against private industry,[276] the government is poorly positioned to make these kinds of judgments.[277] Additionally, hackbacks will work best when responding swiftly, while the hacker is still online.[278]

Second, responding through hackbacks contribute to increasing the cost of hacking in the first place. For any regime governing cross-border hacking, the goal should be raising the net-cost of pernicious hacking to disincentivize the practice. Responding with trade sanctions or other state-centered responses are poor vehicles for delivering this disincentive. If non-state or quasi-non-state actors are performing the hacking, countermeasures in the form of trade sanctions depend on the state adequately shifting the burden of such trade sanctions to those actors in its territory. But there is no guarantee that a state would be willing or able to do so successfully. By contrast, hackbacks are by their very nature directly targeted at the source. If done successfully, any disruption caused by the hackback

273. While there may be judicial remedies for domestic cyberharm, this Note assumes that in the case of cross-border hacking, there are no realistic judicial remedies.

274. Such costs would presumably include not only the costs for intrusion detection and for the actual hacking itself, whether through a contractor or in-house, but also potential liability for damage caused to innocent third parties. *See* Jay P. Kesan & Ruperto P. Majuca, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* (Conf. on Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities, Sept. 8–10, 2005, Oxford Internet Institute, Oxford, UK).

275. *See generally id.* (building a game-theoretic model to find socially optimal scenarios for cyber self-defense); *see also* Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (2010); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429 (2012).

276. In 2011, the White House proposed legislation that would mandate cybersecurity audits for critical national infrastructure (CNI), but the proposal failed to gain traction. *See* Press Release, White House, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

277. One could imagine an economic model to analyze optimal reciprocal hackbacks on a global scale in a similar manner to the Bagwell-Staiger economic model for reciprocal measures in the trade context. *See* Kyle Bagwell & Robert W. Staiger, *An Economic Theory of GATT*, 89 AM. ECON. REV. 215 (1999).

278. *See* Kesan & Majuca, *supra* note 274.

can raise the cost of hacking in the first place.

Third, from an international legal perspective, permitting affected non-state actors to respond maintains symmetry with the allegedly wrongful international act.[279] As we have found, a state is in violation of international law when it fails to exercise due diligence in preventing its territory from being used to cause significant cyber-harm.[280] By responding with "like" behavior—that is, allowing affected private actors to respond—the victim state is temporarily entitled to intentionally cease its due diligence obligation to prevent. From an international law standpoint, then, this method helps ensure that the countermeasures used are truly reciprocal.[281]

Even if we are satisfied that responding with hackbacks is appropriate, there are additional worries that private responses would be *disproportionate* or otherwise excessive.[282] For this reason, any neglect of the duty to prevent must be sufficiently *tailored* to ensure that the countermeasures remain proportionate.

From a legal perspective, there are two important worries about permitting private parties to retaliate. First, firms may respond *excessively* or otherwise disproportionately. Second, firms may respond *poorly* and harm innocent parties. With respect to the first concern, it is important to recognize the asymmetry of interests between the hacker and the retaliating party. The hacker either hopes to obtain confidential information from its target, or it wishes to disrupt or otherwise damage the target. Frequently, however, the retaliator will not share these interests.[283] That said, the proportionality ele-

279. This is especially important in the proportionality context. *See supra* Part III.B.

280. *See supra* Part II.B.2.

281. Indeed, this accords with the Dispute Settlement Understanding's preference for countermeasures in the same sector or agreement of the underlying violation. *See supra* notes 244–45 and accompanying text. For discussion on ensuring that the measures used by private actors are proportionate, see *supra* Part III.B.

282. *See supra* notes 256–260 (proportionality under the ILC conception); *see also supra* note 249 (ICJ's approach in *Gabčíkovo-Nagymaros*).

283. *See* Stewart Baker, *RATS and Poison: Can Cyberespionage Victims Counterhack?*, SKATING ON STILTS (Oct. 13, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/10/us-law-keeps-victims-from-counterhacking-intruders.html (noting that with target counterhacking tools "trashing the attacker's system is dumb; it is far more valuable as an intelligence tool than for any other purpose."). It is rare that a firm would ever be incentivized to respond in a manner disproportionate to the underlying violation. To see why, assume the proper standard for proportionality is the "equality-of-harm" standard used by the DSB. *See supra* notes 244–47 and accompanying text. Recall that under this standard, the arbitrators compare the violation to a "counterfactual" in which the violation is not present. *See* Thomas Sebastian, *The Law of Permissible WTO Retaliation*, *in* THE LAW,

ment of the countermeasures regime behooves the state to ensure that responses are not disproportionate, and the state may have to develop rules, laws, or best practices to ensure private actors are responding proportionately.[284] There is also a risk that firms will fail to target their responses appropriately. This is of particular concern when hackers are utilizing a large number of zombie or bot computers to carry out their hacks, some of which might be utilized by particularly vulnerable targets, such as hospitals.[285] Each of these concerns require that a state considering tailored neglect as a countermeasure to transboundary cyberharm must properly monitor any private actors engaging in retaliatory hacking.

CONCLUSION

Technological hurdles, political realities, and the very nature of the Internet make a national cyberdefense strategy unlikely to be effective or even feasible. Absent miracle-level diplomacy, cyber espionage of private firms is likely only to increase in frequency and severity. Private corporations may increasingly rely on defensive hackbacks to repel cross-border incursions on their networks. While most have assumed this behavior was outside the ambit of public international law, this Note has offered an account of how international law can govern both hacks and hackbacks. Significant harm done to a state's intellectual property should be viewed as "transboundary cyberharm" and can be analyzed under traditional international legal principles, including the due diligence obligation to prevent significant harm to another state's territorial sovereignty, as translated to modern realities. This framework can help us understand the responsibilities and privileges of states when it comes to regulating cyber espionage.

ECONOMICS, AND POLITICS OF RETALIATION IN WTO DISPUTE SETTLEMENT 89, 101 (Chad P. Bown & Joost Pauwelyn eds., 2010). When applying this to your garden-variety APT attack, any metric reveals a detriment that will likely exceed any detriment caused by the counterhack.

284. In its recent report, the White House has already outlined the development of best practices for defense among private industry as a priority. *See* WHITE HOUSE, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, *supra* note 266. Though the report does not mention the development of best practices for offensive maneuvers, there is no reason this cannot be done, along with guidelines, and perhaps sanctions, for disproportionate responses.

285. This is one of Neal Katyal's primary objections. *See* Katyal, *supra* note 108; *see also* Karnow, *supra* note 101, at 89; *see supra* notes 119–21 and accompanying text.

*Jan E. Messerschmidt**

* Head Articles Editor, *Columbia Journal of Transnational Law*; J.D. Candidate, Columbia Law School, 2014; B.A., New York University, 2007. The author would like to thank Professor Matthew C. Waxman for his invaluable guidance, comments, and support throughout the writing process. He is also thankful for input on early drafts by Professor David Pozen and Benjamin W. Schrier. He is also deeply indebted to the entire editorial staff of the *Journal*, with special thanks to Evan Ezray, Sam Levander, Ramya Ravishankar, Jack Schinasi, and Zack Sharpe. Finally, and most importantly, he thanks his parents for their constant and unyielding support.