INTERNATIONAL CYBERTORTS: EXPANDING STATE ACCOUNTABILITY IN CYBERSPACE

Rebecca Crootof[†]

States are not being held accountable for the vast majority of their harmful cyberoperations, largely because classifications created in physical space do not map well onto the cyber domain. Most injurious and invasive cyberoperations are not cybercrimes and do not constitute cyberwarfare, nor are states extending existing definitions of wrongful acts permitting countermeasures to cyberoperations (possibly to avoid creating precedent restricting their own activities). Absent an appropriate label, victim states have few effective and non-escalatory responsive options, and the harms associated with these incidents lie where they fall.

This Article draws on tort law and international law principles to construct a comprehensive system of state accountability in cyberspace, where states are liable for their harmful acts and responsible for their wrongful ones. It identifies international cybertorts—acts that employ, infect, or undermine the internet, a computer system, or a network and thereby cause significant transboundary harm—as distinct from cybercrime and cyberwarfare. Not only does this term distinguish a specific kind of harmful act, it highlights how the principle of state liability for transboundary harms (which holds states accountable for the harmful consequences of both their lawful and unlawful activities) could usefully complement the existing law of state responsibility (which applies only to unlawful state acts). Imposing state liability for international cybertorts minimizes the likelihood that victim states will resort to escalatory responses, increases the chance that those harmed will be compensated, and preserves a bounded grey zone for state experimentation in cyberspace.

---

† Executive Director, Information Society Project; Research Scholar and Lecturer in Law, Yale Law School. For productive conversations and useful insights, many thanks to Dapo Akande, BJ Ard, Jack Balkin, Jack Goldsmith, Claudia Haupt, Ido Kilovaty, Asaf Lubin, Torey McMurdo, Michael Schmitt, Beatrice Walton, Sean Watts, and Sheldon Welton. Earlier drafts were much improved by feedback from presentations at the ISP Fellows Writing Workshop, Andrew Chin's Cyberspace Law course, and the Yale PhDs in Law Tea. As always, many thanks to Douglas Bernstein for thoughtful and clarifying edits.

INTRODUCTION

In 2014, the North Korean "Guardians of Peace" hacker group raided Sony Pictures Entertainment servers and publicized extensive confidential data, including previously-unreleased films, executives' embarrassing personal emails, actors' passports and aliases, and Sony employees' personal and medical information.[1] In response, the United States took the then-unprecedented move of publicly attributing the Guardians' cyberoperations directly to the state of North Korea and imposing new financial sanctions.[2] Experts estimate that the costs of

---

[1] David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ [http://perma.cc/K6WL-QYBS]. This occurred after Sony refused to cancel the planned release of the film *The Interview*, a political satire wherein journalists are recruited by the CIA to assassinate North Korean leader Kim Jong-un. *Id.*

[2] Press Release, U.S. Dep't of Treasury, Treasury Imposes Sanctions Against the Government of the Democratic People's Republic of Korea (Jan. 2, 2015), https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx

the Sony hack include $80 million in direct damages and more than $120 million in indirect damages (such as leaked trade secrets and lost revenue).[3]

Eighteen months later, on the eve of the Democratic National Convention, WikiLeaks released approximately 19,000 emails written by top officials in the Democratic National Committee (DNC) that criticized and mocked then-presidential-hopeful Senator Bernie Sanders, sowing discord in an already-divided political party.[4] A private cybersecurity firm determined that the emails had been obtained by hacker groups associated with the Russian government;[5] months later, the Obama Administration formally attributed the DNC hack to Russia,[6] sparking a debate about whether the hack and subsequent info dump altered the results of the 2016 presidential election. The economic expenses associated with the DNC hack were high; the political costs are impossible to calculate.

Predictably, the Sony hack and DNC hack were popularly termed "cyberwarfare"[7]—and, equally predictably, these char-

---

[http://perma.cc/HUZ8-HEF7]; *see also* Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.b6a3e5d88405 [https://perma.cc/9W36-ZETD] (quoting the co-founder of CrowdStrike's statement that the "public attribution of the attack to North Korea is a watershed moment").

3 Lianna Brinded, *The Interview Tipped to Cost Sony Pictures $200 Million Following Hack and Cancellation*, INT'L BUS. TIMES (Dec. 18, 2014, 4:42 PM), http://www.ibtimes.co.uk/interview-tipped-cost-sony-pictures-200m-total-following-hack-cancellation-1480157 [http://perma.cc/A2ZM-6YMV].

4 Spencer Ackerman & Sam Thielman, *US Officially Accuses Russia of hacking DNC and Interfering with Election*, GUARDIAN (Oct. 8, 2016, 9:09 AM), https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election [http://perma.cc/AU7B-LN76]; Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ [http://perma.cc/85PE-992S].

5 Ackerman & Thielman, *supra* note 4.

6 David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES (Oct. 7, 2016), https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html?mcubz=0 [https://perma.cc/TV5D-7RFL]. While Russia has repeatedly denied having orchestrated the attacks, in May 2017 Russian President Vladimir Putin made the startling suggestion that "patriotically minded" private Russia hackers could have meddled in the U.S. election. Andrew Higgins, *Maybe Private Russian Hackers Meddled in Election, Putin Says*, N.Y. TIMES (June 1, 2017), https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html?mcubz=0 [https://perma.cc/E856-UD9V].

7 With regard to the Sony hack, former Speaker of the House Newt Gingrich tweeted, "No one should kid themselves. With the Sony collapse America has lost

acterizations were followed by a spate of academics and specialists clarifying that the hacks did not satisfy the legal requirements for that title.[8] But if these cyberoperations were not cyberwarfare, what were they? They were cyberespionage and transnational cybercrime—but they were also something more. Unlike most cyberespionage, the stolen information was intentionally publicized with an apparent intent to cause harm. Unlike most transnational cybercrimes, the cyberoperations were state-sponsored—and while individuals in the Guardians of the Peace and Russian hacker groups can theoretically be held criminally liable, North Korea and Russia cannot.[9] Some

---

its first cyberwar. This is a very very dangerous precedent." Newt Gingrich (@newtgingrich), TWITTER (Dec. 17, 2014, 2:05 PM), https://twitter.com/newtgingrich/status/545339074975109122 [http://perma.cc/389W-5F7T]. Senator John McCain described the DNC hack as an "act of war." Theodore Schleifer & Deirdre Walsh, *McCain: Russian Cyberintrusions an 'Act of War,'* CNN (Dec. 30, 2016, 8:27 PM), http://www.cnn.com/2016/12/30/politics/mccain-cyber-hearing/ [http://perma.cc/8KE2-MMTN].

8 *See, e.g.*, Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SECURITY (Jan. 5, 2017, 8:01 AM), https://www.justsecurity.org/35999/international-law-response-russian-election-interference/ [http://perma.cc/S3KM-B8JC] (asserting that the DNC hack "would [not] amount to an 'act of war' in any legal sense of what that term might mean"); Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014, 9:29 AM), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ [http://perma.cc/6YPY-XD69] (noting that the Sony hack was "not at the level most experts would consider an armed attack"); *see also* Peter W. Singer & Allan Friedman, *5 Lessons from the Sony Hack*, CNN (Dec. 17, 2014, 6:00 PM), http://www.cnn.com/2014/12/17/opinion/singer-friedman-sony-hacking-lessons/index.html [http://perma.cc/6X6X-XUDR] ("[The Sony hack] has often been lumped in with stories ranging from run of the mill online credit card theft to the Target, Home Depot and JP Morgan breaches to the time that Iranian-linked hackers allegedly 'erased data on three-quarters of Aramco's corporate PCs.' . . . It's a lot like lumping together every incident in New York that involves a gun, whether it's a bank robbery, a murder or a football player accidentally shooting himself.").

9 The 2001 Council of Europe Convention on Cybercrime establishes "a common criminal policy aimed at the protection of society against cybercrime." Convention on Cybercrime, Council of Europe, pmbl., Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004). As of September 2017, fifty-five states have ratified or acceded to the Convention, and an additional four have signed it. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL EUR., TREATY OFF., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185& CM=8&DF=28/10/2010&CL=ENG [https://perma.cc/5UTL-2PB7]. The Convention creates no international law crimes; rather, it creates international law obligations to enact domestic law and render mutual assistance. And, as with most criminal law regimes, this treaty is meant to govern the unlawful actions of individuals, not of states. All in all, it is wholly inadequate for addressing state-sponsored cyberoperations—notwithstanding the fact that, with a few notable (and contested) exceptions, the vast majority of significantly harmful and intrusive cyberoperations appear to have been sponsored by states. Furthermore, attempts to investigate and prosecute individuals for transnational cybercrimes under the treaty have not been markedly successful. *Cf.* Michael J. Glennon, *State-level Cyber-*

have suggested that these cyberoperations might be internationally wrongful acts—violations of a state's international obligations—but scholars are divided on that question.[10] Importantly, the United States never claimed either hack was a violation of international law—instead, as evidenced by then-President Obama's description of the Sony hack as "cyber-vandalism,"[11] states are casting about for a way to characterize such acts negatively without explicitly labeling them as unlawful (and thereby setting a precedent that might limit their own cyberoperations). In short, despite being widely recognized as important and possibly even world-altering,[12] there is no obviously accurate term for cyberoperations like the Sony and DNC hacks.[13]

---

security, POL'Y REV., Feb.–Mar., 2012, at 85, 89 (noting that the Convention's "provisions have proven notoriously ineffective as nations have struggled to find the common ground necessary to keep pace with evolving threats").

10 The Sony hack might be considered a violation of U.S. sovereignty, insofar as there was manipulation of cyber infrastructure and the insertion of malware. Schmitt, *supra* note 8. It is less clear if the DNC hack could be similarly characterized, given that compromising computer systems and stealing data might be considered routine state practice in cyberspace. Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SECURITY (Oct. 14, 2016, 8:48 AM), https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/ [http://perma.cc/3N3E-R54E]. Neither cyberoperation would seem to be sufficiently coercive to meet the standard required for prohibited intervention. *See id.* (explaining that, to be a prohibited intervention, an "operation must force the target State into a course of action it would not otherwise undertake").

11 Chris Strohm, *North Korea Web Outage Response to Sony Hack, Lawmaker Says*, BLOOMBERG (Mar. 17, 2015, 5:49 PM), http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says [http://perma.cc/V3LH-5M64]. Similarly, the Obama administration characterized the DNC hack as a violation of international norms rather than of international law. Press Release, Office of the Press Sec'y, White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [https://perma.cc/F7G9-MJTL].

12 *See, e.g.*, Michael Morell & Suzanne Kelly, *Fmr. CIA Acting Dir. Michael Morell: "This Is the Political Equivalent of 9/11*," CIPHER BRIEF (Dec. 11, 2016), https://www.thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091#.WE6RWJk6AUU.twitter [http://perma.cc/Z5KQ-E8KG] (characterizing the DNC hack as "an existential threat to [the American] way of life").

13 The Sony hack has also been described as an act of cyberterrorism. *See* Ellen Nakashima, *White House Says Sony Hack Is a Serious National Security Matter*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html?utm_term=.a270fdd4a97e [http://perma.cc/9DGP-CC9P]. However, as with its root term "terrorism," it is controversial whether a state can engage in cyberterrorism. *Compare* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND.

In addition to being difficult to classify, cyberoperations like the Sony and DNC hacks often cause significant harms. According to a 2014 PricewaterhouseCoopers survey, the number of institutions reporting cyberoperations costing them more than $20 million in losses increased 92% from 2013 to 2014, with an 86% increase in the number reporting attacks by nation-states.[14] Experts estimate that malicious cyberoperations cost the U.S. economy between $120 and $167 billion in 2015 alone;[15] others calculate that they will cost global businesses more than $6 trillion annually by 2021.[16]

The Sony hack, DNC hack, and other recent malicious cyberoperations have highlighted a significant gap in the international law of cyberspace: states are not being held accountable for these kinds of harmful cyberoperations, in part because classifications created in physical space do not map well onto the cyber domain and in part because states appear unwilling to extend existing definitions of wrongful state acts to these activities. As a result, states victim to injurious and invasive cyberoperations currently have few non-escalatory responsive options, and the harms associated with these incidents tend to lie where they fall.

To address this growing issue, this Article draws on tort law and international law principles to construct a comprehensive state accountability regime in cyberspace, where states are both liable for their harmful acts and responsible for their wrongful ones. It identifies international cybertorts—acts that employ, infect, or undermine the internet, a computer system, or a network and thereby cause significant transboundary harm—as a distinct kind of cyberoperation, and in doing so

---

J. TRANSNAT'L L. 57, 63 (2010) (asserting that cyberterrorism does not include state actions), *with* Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 809 (2010) (citing Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 404–05 (2007) (noting view that states can engage in cyberterrorism)).

14 PRICEWATERHOUSECOOPERS, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD 10, 16 (2014), http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf [http://perma.cc/FJ37-BMTC].

15 THE GEORGE WASH. UNIV. CTR. FOR CYBER & HOMELAND SEC., INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 3 (2016) [hereinafter ACTIVE DEFENSE REPORT].

16 CYBERSECURITY VENTURES, HACKERPOCALYPSE: A CYBERCRIME REVELATION 6 (2016), http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [http://perma.cc/Q7YP-XDGA] (noting that this assessment "include[s] damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm").

distinguishes and clarifies the boundaries of cybercrime and cyberwarfare. Recognizing this new category also highlights how the principle of state liability for transboundary harms (which holds states accountable for the harmful consequences of both their lawful and unlawful activities) could usefully complement the existing law of state responsibility (which applies only to unlawful state actions).[17]

Delineating international cybertorts creates a useful intermediate space between unproblematic state activity in cyberspace and cyberwarfare. Labeling a harmful cyberoperation an international cybertort does not mean that it was necessarily unlawful; rather, it puts the perpetrator on notice that it might be liable for associated injuries. As a result, imposing state liability for international cybertorts preserves a bounded grey zone for state experimentation, while simultaneously minimizing the likelihood that states harmed by cyberoperations will resort to escalatory self-help measures and increasing the likelihood that victims will be compensated.

This proposal has precedent in international law: various treaties describe liability standards for different kinds of conduct,[18] and states regularly set up institutions to evaluate state liability for harms and settle claims in other contexts.[19] Furthermore, this Article's proposals could be immediately incor-

---

17 On this point, I owe a great debt to conversations with Beatrice Walton, who has since published the first piece of scholarly writing defining the concept of state liability in international law and evaluating how it applies to cyberoperations. Beatrice A. Walton, Note, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460, 1478–88 (2017).

18 *See, e.g.*, Convention on the International Liability for Damage Caused by Space Objects art. II, Mar. 29, 1972, 24 U.S.T. 2389, 2392, 961 U.N.T.S. 187, 189 ("A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight.").

19 For example, many military powerhouses already voluntarily compensate victims of their actions in armed conflicts with *ex gratia* payments. *See, e.g.*, Paul von Zielbauer, *Confusion and Discord in U.S. Compensation to Civilian Victims of War*, N.Y. TIMES (Apr. 12, 2007), http://www.nytimes.com/2007/04/12/world/americas/12iht-abuse.1.5246758.html [http://perma.cc/CMC8-3FWJ] (noting that, between 2001 and the spring of 2007, the United States "paid more than $32 million to Iraqi and Afghan civilians for noncombat-related killings, injuries and property damage"); *see also* Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347, 1393 (2016) (discussing the U.S. Foreign Claims Act and NATO's Status of Forces Agreement (SOFA) as examples of states voluntarily committing to compensate the victims of their activities).

In other situations, compensation claims are settled after protracted legal proceedings. For example, after more than five years of litigation, the United States settled a claim with Iran on behalf of the victims of the downing of Iran Air Flight 655 for $61.8 million. Aerial Incident of 3 July 1988 (Iran v. U.S.), Settlement Agreement, 35 I.L.M. 553, 553 (1996).

porated within the existing international enforcement mechanisms. Ideally, however, states would create an independent institution with the expertise and investigative resources to impartially assess state accountability in cyberspace, the flexibility to adapt to changing technologies, and the enforcement authority to deter states from engaging in inappropriate and escalatory self-help. This would not entirely eliminate legal grey zones—new technological developments, state reluctance to disclose technological capabilities, and state interest in preserving some unregulated space will ensure there is plenty of grist for the academic mill—but an independent institution would increase the likelihood that the international law of cyberspace develops in a cohesive manner.

Part I reviews how the architecture of cyberspace and the structure of the modern international legal order—particularly its restrictions on self-help measures—has resulted in a lack of effective, non-escalatory deterrents to increasingly harmful but difficult-to-classify cyberoperations. Part II identifies international cybertorts as a distinct class of cyberoperation; clarifies its relationship with cyberwarfare, transnational cybercrime, data destruction, ransomware, cyber exploitation, and cyberespionage; and proposes that states be held accountable for their cybertorts under the principle of state liability for transboundary harms. Part III reviews the law of state responsibility, discusses why cyberspace facilitates certain kinds of internationally wrongful acts, and argues for minimizing resort to claims of state responsibility (with its attendant risk of conflict escalation) in light of the possibility of state liability. Part IV considers how best to develop a comprehensive accountability regime for state activity in cyberspace.

I
A PROBLEM WITHOUT A NAME

The architecture of cyberspace favors attackers, preventing states from enacting effective defenses; simultaneously, existing international law limits victim states' recourse to effective and non-escalatory ex post deterrents. This combination has resulted in an increase in costly and invasive state-sponsored cyberoperations, evidenced by the following symptomatic examples.[20]

---

20 As Sean Watts has observed, "[i]n addition to being highly feasible and often inexpensive, low-intensity cyber operations offer attractive prospects for anonymity, appear to frustrate attack correlation by targets, and may also reduce the likelihood of provoking severe retaliation. In short, low-intensity cyber opera-

In October 2012, Chinese government officials warned the *New York Times* that its investigation into how relatives of China's Prime Minister Wen Jiabao had recently accumulated billions of dollars would "have consequences."[21] Four months later, the paper publicized that Chinese hackers had infiltrated its computer systems.[22] While they could have utterly destroyed the *Times*'s network infrastructure, the hackers instead appeared to be looking for information as to sources in the investigation.[23] The intrusion was quarantined and eliminated only after the *Times* hired a private company that specialized in security breaches, set up new defenses, and replaced all compromised computers.[24]

In December 2014, the Sands Casino in Las Vegas was attacked, allegedly by Iranian hackers: computers and servers shut themselves down and hard drives were wiped.[25] This was the first known case of a cyberoperation targeting an American business designed to destroy (rather than spy or steal)—and the attack was almost undoubtedly retaliation for comments that its CEO Sheldon Adelson had made about nuking Tehran.[26] The immediate costs of lost equipment and data were estimated at $40 million.[27]

On the April 2015 premiere date of TV5Monde, a new French broadcast channel, allegedly-Russian cyberoperations targeted and disrupted the "internet-connected hardware that controlled the TV station's operations."[28] The financial costs of the attack ran to €5 million in 2015, and TV5Monde has spent

---

tions offer states appealing opportunities to degrade adversaries while avoiding the likely strategic and legal costs of massively destructive cyber attacks." Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 250 (Jens David Ohlin et al. eds., 2015).

21 Nicole Perlroth, *Hackers in China Attacked the Times for Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?mcubz=0 [https://perma.cc/63KC-7K4V].

22 *Id.*

23 *Id.*

24 *Id.*

25 Benjamin Elgin & Michael Riley, *Now at the Sands Casino: An Iranian Hacker in Every Server*, BLOOMBERG (Dec. 12, 2014, 3:48 PM), http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas [http://perma.cc/5FYJ-PEPX].

26 *Id.*

27 *Id.*

28 Gordon Corera, *How France's TV5 Was Almost Destroyed by 'Russian Hackers*,*'* BBC NEWS (Oct. 10, 2016), http://www.bbc.com/news/technology-37590375 [http://perma.cc/J8FQ-5CRV].

over €3 million every year since for new protections.[29] These costs, however, were cheap compared to the possibility of the entire business being destroyed. TV5Monde's director-general recalled that, due to the risks of customer cancellations, "We were a couple of hours from having the whole station gone for good."[30]

Other costly and intrusive state-sponsored cyberoperations include the U.S.- and Israeli-linked 2010 Stuxnet attack,[31] the 2012 Iranian-linked attack on a Saudi Arabian oil company,[32] the 2015 Russian-linked attack on the Ukrainian electrical grid,[33] the 2016 U.S. internet shutdown[34]—and, of course, the 2014 Sony hack and 2016 DNC hack.

States and scholars are looking to international law for guidance on how to lawfully respond to these harmful cyberoperations. But international law has little to say on the subject—except to limit a victim state's lawful unilateral self-help options.

A. Modern International Law's Limitations on Self-Help

Limited state recourse to self-help measures is a feature of the modern international legal order, which prioritizes international peace over perfect enforcement. States are expected to let minor slights and violations of international law go unaddressed to avoid perpetuating cycles of escalatory self-help.

This was not always the case. Historically, international law was created and enforced through self-help measures, with states often using military force to settle a wide range of disputes.[35] "Self-help" refers to "private actions taken by those

---

29 *Id.*

30 *Id.*

31 Michael B. Kelley, *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013, 12:58 PM), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 [https://perma.cc/S45P-UX6H].

32 Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?mcubz=3 [https://perma.cc/G638-H8CA].

33 Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [http://perma.cc/8Y58-HM2H].

34 Robert Windrem et al., *Who Shut Down the Internet Friday?*, NBC NEWS (Oct. 21, 2016, 7:21 PM), https://www.nbcnews.com/news/us-news/who-shut-down-u-s-internet-friday-n671011 [https://perma.cc/KAW3-T3NB].

35 *See* OONA A. HATHAWAY & SCOTT SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD (2017).

interested in [a] controversy to prevent or resolve disputes without official assistance of a governmental official or disinterested third party."[36] The legitimacy of self-help has long been recognized, particularly in environments where there is no authoritative lawmaker or law enforcer.[37]

Allowing individual actors to unilaterally address wrongdoing has a number of benefits: it "may serve to deter such wrongdoing from occurring in the first place, reduce administrative costs, promote autonomy- or sovereignty-related values, and facilitate speedier redress."[38] At a larger level, self-help "might serve to facilitate the maintenance of cooperative relations, mitigate feelings of alienation from the law, or generate deeper internalization of first-order legal norms."[39]

Self-help systems, however, are inherently unstable and prone to conflict escalation. Because self-helpers judge their own cause, "[t]here is ample reason to worry that they will misconstrue the law along the way—not just, or even primarily, on account of bad faith, but on account of motivated cognition and reliance on congenial interpretive methods or theories of law."[40] Self-help regimes also disproportionately favor the powerful and foster vicious cycles of attacks and counterattacks.

Given the likelihood that it will result in inappropriate responses and conflict escalation, legal systems often limit recourse to self-help. This was an animating reason for the formation of the U.N. Charter, which sharply restricts the use of violent self-help, as well as the development of the law of countermeasures, which limits state recourse to non-violent self-help measures.

1. *Charter Restrictions on the Use of Force*

Article 2(4) of the U.N. Charter prohibits states from unilaterally using force: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United

---

36 Celia R. Taylor, *Self-Help in Contract Law: An Exploration and Proposal*, 33 WAKE FOREST L. REV. 839, 841 (1998).

37 *Id.* at 844 ("Prior to the existence of legal institutions to dictate rules of behavior and state authorities to enforce them, all social relations were a form of self-help.").

38 David E. Pozen, *Self-Help and the Separation of Powers*, 124 YALE L.J. 2, 49 (2014).

39 *Id.*

40 *Id.* at 50 (footnote omitted).

Nations."[41] Instead of taking matters into their own hands, states are expected to pursue institutionalized means of resolving major disputes[42] and to let minor ones go unpunished.

There is one express exception to Article 2(4)'s general prohibition on unilateral state recourse to force. Article 51 provides: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[43] The threshold for an "armed attack" is generally understood to be higher than that required for a use of force,[44] though the U.S. minority opinion that the two terms are essentially co-extensive[45] has created a legal debate that has extended to assessments of the law of cyberspace.[46] But while there is disagreement over where the threshold lies, it is now generally accepted that states may unilaterally use defensive force in response to cyber-enabled armed attacks. If an act does not clear the armed attack threshold, victim states can still unilaterally take non-violent responsive measures, subject to the limits discussed below.

2. *Customary Limits on the Use of Countermeasures*

The law of countermeasures developed in the shadow of the U.N. Charter as a means by which states victim to "below the threshold" acts could still take unilateral action to bring international law violators back into compliance. Countermeasures are "measures that 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

---

41 U.N. Charter art. 2(4); *see also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 148 (Dec. 19) ("The prohibition against the use of force is a cornerstone of the United Nations Charter.").

42 For example, states may lawfully use force against another state after having procured an authorizing Security Council resolution. U.N. Charter art. 39.

43 *Id.* art. 51.

44 *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27).

45 *See, e.g.*, Harold Hongju Koh, International Law in Cyberspace, Remarks to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1 (2012).

46 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 69 cmt. 7 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0] (acknowledging the U.S. minority view).

to procure cessation and reparation."[47] For example, an injured state may suspend transit or trade rights with a state in violation of a treaty until it ceases the wrongful act or makes appropriate reparation.[48]

In keeping with the U.N. Charter's general bent towards minimizing escalation, violent countermeasures are not permitted: "Countermeasures shall not affect . . . the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations."[49] Thus, reciprocal violent countermeasures in response to a violation of Article 2(4) would also violate Article 2(4).[50]

Furthermore, even the use of non-violent countermeasures is strictly circumscribed. There are many situations in which countermeasures cannot be used at all,[51] and when they are allowed, they must satisfy a number of requirements to be lawful. To name just a few, countermeasures must be temporary in their effects, comply with the principles of necessity and proportionality, and be designed to induce compliance with international law.[52] Importantly, countermeasures must be taken "to procure cessation and reparation" of an internationally wrongful act—not to punish.[53]

In contrast to the strict restrictions on the use of force and countermeasures, states may always employ retorsions to at-

---

47 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Int'l L. Comm'n, Rep. on the Work of Its Fifty-Third Session, ch. 2 cmt. 1, U.N. Doc. A/56/10 (2001) [hereinafter Draft Articles].

48 *Id.* art. 49 cmt. 5.

49 *Id.* art. 50(1)(a); *see also id.* art. 59 ("These articles are without prejudice to the Charter of the United Nations."); *id.* ch. 2 cmt. 6 (noting that the Articles apply only to "non-forcible countermeasures"); *id.* art. 50 cmt. 4 (excluding "forcible measures from the ambit of permissible countermeasures"); TALLINN MANUAL 2.0, *supra* note 46, r. 22 cmt. 11 (noting that the majority of experts consider "the obligation to refrain from the use of force" to be "a key limitation on an injured State when conducting countermeasures").

50 *See* Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, *in* NATO CCD COE PUBL'NS, 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 39, 48 (2014). *But see* TALLINN MANUAL 2.0, *supra* note 46, r. 22 cmts. 12–14 (acknowledging a minority view that "forcible countermeasures are appropriate in response to a wrongful use of force that itself does not qualify as an armed attack" is supported by Judge Simma's separate opinion in the *Oil Platforms* judgment).

51 For example, a victim state may not use countermeasures in response to an internationally wrongful act that has ceased and is unlikely to be repeated, Draft Articles, *supra* note 47, arts. 49(2), 52(3)(a); when the internationally wrongful act has ended and the issue is pending before a third-party dispute settlement procedure, *id.* art. 52(3); and countermeasures cannot violate fundamental human rights, *jus cogens* norms, the prohibition on belligerent reprisals, or dispute settlement procedures, *id.* art. 50(1).

52 *Id.* art. 49(3) cmts. 6–7.

53 *Id.* ch. 2 cmt. 1.

tempt to alter another state's behavior.[54] While countermeasures are acts that would be unlawful but for the fact that they are taken to restore order (like reciprocal treaty breaches), retorsions are politically unfriendly but always lawful self-help measures (like discontinuing development aid, declaring a diplomat *persona non grata*, or imposing unilateral sanctions).[55]

In short, states may unilaterally use defensive force in response to armed attacks, states may sometimes engage in countermeasures to correct another state's unlawful acts, and states may always employ retorsions in the attempt to alter another state's behavior. However, these rules and enforcement mechanisms were developed in the physical world and founded on assumptions that do not translate well to cyberspace, resulting in a general lack of credible deterrents to harmful state-sponsored cyberoperations.

B. The Need for Effective, Non-Escalatory Deterrents

Deterrence theory is based on the presumption that certain actions will either be unsuccessful or lead to consequential and painful responses.[56] Deterrence by denial in cyberspace is of limited utility, as defensive measures can only do so much in an environment that favors attackers. Meanwhile, international legal constraints on self-help measures become even more restrictive when translated to cyberspace, limiting the unilateral ex post options of a state victim to a harmful or invasive cyberoperation.

1. *Practical Limits of Deterrence by Denial*

A state or non-state entity should be expected to take basic precautions to avoid being too easy a target.[57] The United

---

54 *Id.* ch. 2 cmt. 3.

55 *Id.* The public U.S. response to the Sony hack would qualify as a retorsion. *Cf.* Dan Roberts, *Obama Imposes New Sanctions Against North Korea in Response to Sony Hack*, GUARDIAN (Jan. 2, 2015, 4:08 PM), https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview [http://perma.cc/L63B-2QWF] ("The US has imposed economic sanctions against several North Korean government agencies and senior officials in retaliation for the country's alleged role in hacking Sony Pictures' systems and threatening US moviegoers.").

56 The most extreme version of this is "mutually assured destruction," where the threat of a full-scale use of nuclear weapons by opposing sides would result in the complete annihilation of both (and, possibly, the rest of the world).

57 At present, this is not a recognized formal duty under international law, though there is growing sympathy for the concept of cyber due diligence—a requirement to not allow harm to emanate from state territory. Should a norm of cyber due diligence be recognized, cybersecurity measures might be requirements (as opposed to best practices). *See infra* Part II(C)(3)(b).

States in particular has emphasized the importance of "deterrence by denial"—in other words, engaging in better cybersecurity practices and beefing up defenses.[58]

Deterrence by denial, however, offers limited protection in the cyber context. Defenders are playing an elaborate game of whack-a-mole, where a single missed attack can have devastating effects. Further, while cybersecurity good practices are important and while there are some justifications for holding states accountable for egregiously poor cybersecurity,[59] overemphasizing a due diligence requirement risks focusing more on the culpability of the entity that left the door unlocked than of the entity that trespassed and burglarized the building.

Lastly, overreliance on contemporaneous defense invites many of the problems associated with self-help measures. The speed of cyber will nearly always require that in-the-moment defenses be automated or autonomous.[60] In most circumstances, a particular cyberoperation will be neutralized by a defense system long before a human being even knows it was attempted. As long as defensive measures are primarily passive and simply shield the target network or repair damage, the lack of human input is relatively unproblematic. But active defenses are a different story. Active defenses can be loosely defined as "a set of operational, technical, policy, and legal measures" that "captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense."[61] These might include both "technical interactions between a defender and an attacker" and "operations that enable defenders to collect intelligence on threat actors and

---

58 *See* U.S. DEP'T OF DEF. SCI. BD., TASK FORCE ON CYBER DETERRENCE 6 (2017) ("Deterrence by denial operates through a combination of defenses and resilience to attack, so that the adversary understands that it will not succeed in the aims of its contemplated cyber attack.").

59 *See* Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 491–99 (2015) (arguing for imposing legal and technological responsibilities on states that are or may be the target of harmful cyberoperations).

60 *See* Eric Messinger, *Is It Possible to Ban Autonomous Weapons in Cyberwar?*, JUST SECURITY (Jan. 15, 2015, 9:27 AM), https://www.justsecurity.org/19119/ban-autonomous-weapons-cyberwar/ [http://perma.cc/2G45-F7LQ]; *see also* Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 CARDOZO L. REV. 1837, 1864–65 (2015) (distinguishing inert, automated, semi-autonomous, and autonomous weapon systems). Unsurprisingly, states and industry are pouring money into developing autonomous cyberdefenses. *See* Billy Mitchell, *DARPA Kicks Off Two-Year Long Autonomous Cybersecurity Tournament*, FEDSCOOP (June 3, 2014), http://fedscoop.com/darpa-kicks-two-year-long-autonomous-cybersecurity-tournament/ [http://perma.cc/LJB6-74HM].

61 ACTIVE DEFENSE REPORT, *supra* note 15, at 1, 9 (emphasis omitted).

indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors."[62] At the far end of the spectrum, some active defenses risk crossing the line into uses of force. If defenses are active and entirely automated or autonomous, it is easy to imagine an exchange of attacks and counter-attacks that quickly escalates into warfare.[63]

Nor are states the only players. Given that the majority of cyberoperations target private sector entities, some cybersecurity experts are suggesting that industries take a more proactive approach to cyberdefense.[64] The more non-state entities employ active defenses without guidance from states, however, the more likely they are to respond in ways that implicate national security and foreign relations concerns and increase the risk of unintended conflicts.[65] For example, in response to a targeted malware attack termed Operation Aurora, Google appears to have gained unauthorized access to Taiwanese computers believed to be under the control of Chinese entities—which could be interpreted as a violation of the Computer Fraud and Abuse Act and which might have had problematic political implications.[66]

---

62 *Id.* at 9 (emphasis omitted).

63 This was a foundational assumption in an entire genre of science fiction novels written or movies produced during the Cold War. *E.g.*, MORDECAI ROSHWALD, LEVEL 7 (1959); WARGAMES (United Artists 1983).

64 *See, e.g.*, Ariel Rabkin & Jeremy A. Rabkin, *Enhancing Network Security: A Cyber Strategy for the Next Administration* 10–11 (Am. Enter. Inst., Working Paper No. 2016-01, 2016), https://www.aei.org/wp-content/uploads/2016/05/Enhancing-network-security.pdf [https://perma.cc/YCZ2-K27X] (arguing that private firms should be given the latitude to experiment with active countermeasures to more effectively safeguard American-based networks).

65 Accordingly, many proposed active defenses should only be taken by private sector entities working in close collaboration with government. *See* Nuala O'Connor, *Appendix I: Additional Views of Nuala O'Connor*, *in* ACTIVE DEFENSE REPORT, *supra* note 15, at 39, 40.

66 *Id.* at 14, 40. Given the many benefits and risks associated with private sector active defense, some have proposed a middle path, with specific limitations on and incentives for appropriate private use of active defenses. *See, e.g.*, WYATT HOFFMAN & ARIEL E. LEVITE, PRIVATE SECTOR CYBER DEFENSE: CAN ACTIVE MEASURES HELP STABILIZE CYBERSPACE? 33–39 (2017) (proposing set of principles to guide conduct of private firms engaging in active cyber defense). In 2017, Representative Tom Graves released a draft "Active Cyber Defense Certainty (ACDC) Act" that would permit limited private defensive measures in cyberspace. Active Cyber Defense Certainty Act – 2.0 (Discussion Draft), https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf [http://perma.cc/649R-TSG2].

2. *Practical and Legal Limits of Deterrence by Punishment*

The risks and insufficiency of deterrence by denial suggests the need for a more traditional conception of "deterrence by punishment." In other words, in the absence of effective ex ante defenses, states need strong ex post deterrents. But deterrence strategies developed in physical space do not always translate well to the cyber domain.[67]

First, there is the attribution problem. If a victim state cannot quickly and reliably identify the actual perpetrator, it will not be able to take timely and appropriate responsive actions. While eventual attribution of a cyberoperation is becoming more feasible (especially as state-sponsored cyberoperations commonly rely on previously-used architectures), it is still nearly impossible to identify the actual perpetrator immediately.[68] This difficulty is compounded when a state acts through a non-state actor. Consider the attack on TV5Monde: the hackers claimed to be members of a group called the Cyber Caliphate and implied that they were linked to the Islamic State; later evidence suggests that the actual perpetrators were a group of Russian hackers known as APT 28 or "Fancy Bear" (the same group likely responsible for the DNC hack).[69] More recently, the NATO Cooperative Cyber Defence Centre of Excellence concluded that the NotPetya malware, which initially appeared to be created by common cybercriminals "was probably launched by a state actor or a non-state actor with support or approval from a state."[70] It reasoned that the operation was likely too complex to have been orchestrated by unaffiliated hackers and that the ransomware collection method "was so poorly designed that the ransom

---

67 *See* MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 39–41 (2009).

68 *See* Kenneth Anderson, *Comparing the Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapon Systems*, HOOVER INSTITUTION: THE BRIEFING (Feb. 27, 2015), http://www.hoover.org/research/comparing-strategic-and-legal-features-cyberwar-drone-warfare-and-autonomous-weapon-systems [http://perma.cc/K3AV-5HH4] ("Technical experts suggest that attribution is becoming more feasible in cyberattacks, though speed of attribution—and, therefore, meaningful response—remains an obstacle.").

69 Corera, *supra* note 28; *see also* Ackerman & Thielman, *supra* note 4 (equating APT 28 and "Fancy Bear" and discussing the DNC hack).

70 *NotPetya and WannaCry Call for a Joint Response from International Community*, NATO CCD COE (June 30, 2017), https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html [http://perma.cc/33VD-TLWK] [hereinafter *NotPetya Joint Response*].

would probably not even cover the cost of the operation."[71] However, at the time of the writing, it had not publicly attributed the cyberoperation to a specific state.[72]

Even if both the cyberoperation and perpetrator are reasonably identifiable, the intended effect or message of a cyberoperation is often unclear. For example, in August 2016, a Twitter account associated with state-sponsored Russian hackers posted a link to a cache of computer codes outlining hacker tools allegedly stolen from the Equation Group, a hacker group long associated with the U.S. National Security Agency (NSA).[73] In a series of tweets, Edward Snowden discussed why this disclosure might have far-reaching foreign policy implications:

> Circumstantial evidence and conventional wisdom indicate Russian responsibility [for the hack]. Here's why that is significant: This leak is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server. That could have significant foreign policy consequences. Particularly if any of those operations targeted US allies. Particularly if any of those operations targeted elections. Accordingly, this may be an effort to influence the calculus of decision-makers wondering how sharply to respond to the DNC hacks. TL;DR: This leak looks like a

---

71 *Id.*; *see also id.* (quoting Lauri Lindström, a NATO CCD COE Strategy Branch researcher, as stating that NotPetya is "likely . . . a declaration of power—demonstration of the acquired disruptive capability and readiness to use it").

72 Others have taken the analysis a step further, arguing that given that 60% of infected machines are in Ukraine and that the attack began the day before the Ukrainian Constitution Day, the attack was likely politically motivated. Lee Mathews, *The NotPetya Ransomware May Actually Be a Devastating Cyberweapon*, FORBES (June 30, 2017), https://www.forbes.com/sites/leemathews/2017/06/30/the-notpetya-ransomware-may-actually-be-a-devastating-cyberweapon/#6ef1c94f39e8 [http://perma.cc/YS9C-D359]. While this has caused some to suggest Russia was responsible for the attacks, others are more reserved: Brian Lord, former deputy director for intelligence and cyber operations at the U.K. Government Communications Headquarters and currently the managing director for cyber and technology at PGI Cyber, noted that "[t]here's something about the blatantness of hitting Ukraine that doesn't sit well with me about this being a Russian attack." Sheera Frenkel, Mark Scott & Paul Mozur, *Mystery of Motive for a Ransomware Attack: Money, Mayhem or a Message?*, N.Y. TIMES (June 28, 2017), https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html?mcubz=0 [http://perma.cc/29WW-ZT4G].

73 Russell Brandom, *The Shadow Brokers Hack Is Starting to Look Like Russia vs. NSA*, VERGE (Aug. 17, 2016, 1:40 PM), https://www.theverge.com/2016/8/17/12519804/shadow-brokers-russia-nsa-hack-equation-group [https://perma.cc/WGW8-HDLQ].

> somebody sending a message that an escalation in the attribution game could get messy fast.[74]

This leak could have been, as Snowden hypothesized, a threat or form of blackmail; it could also have been a provocation, information warfare intended to discredit the NSA, propaganda for Russian or other audiences, or a response to some other action (either in cyberspace or physical space, publicly known or not). The proper response would differ depending on what the action was or was meant to be—but without knowing the intent of the action, it is difficult for states to respond appropriately. Furthermore, while the disclosure of the NSA hack was apparently deliberate, it is possible to imagine a scenario where malware intended for cyberespionage malfunctioned and caused an inadvertently harmful result. In an ideal world, the victim state would react differently to a mistake than to intentional destruction; in this one, a victim state might not be able to make that distinction.

Finally, in situations where a victim state knows it has been subject to an invasive cyberoperation and can reasonably identify both the state perpetrator and the purpose of the action, there are fewer lawful responsive options available in the cyber domain than in physical space. As discussed above, modern international law discourages violent state vigilantism to avoid the risk of conflict escalation.[75] States are permitted to take unilateral self-help measures subject to strict legal limitations—but those limitations prevent most forms of state self-help in response to harmful cyberoperations.

Should a cyberoperation constitute an armed attack, the victim state can use defensive force in response, but most cyberoperations are not sufficiently destructive to meet the armed attack threshold.[76] States victim to "below the threshold" cyberoperations may theoretically employ countermeasures and retorsions to alter a suspected perpetrator's behavior,[77] but absent amendment or significant reinterpretation, these options have limited efficacy.

---

74 Swati Khandelwal, *The NSA Hack – What, When, Where, How, Who & Why?*, HACKER NEWS (Aug. 17, 2016), https://thehackernews.com/2016/08/nsa-hack-russia-leak.html [http://perma.cc/K9KW-QPGV].

75 *See supra* subpart I.A; *see also* TALLINN MANUAL 2.0, *supra* note 46, r. 20 cmt. 16 (discussing limits on countermeasures and noting that countermeasures "present a risk of escalation").

76 *See infra* text accompanying notes 110–14.

77 *See* Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 857–59, 857 n.170, 866 (2012) (suggesting that the law of countermeasures might be relevant in cyberspace and noting that victim states may lawfully

Because self-help measures are meant to be a last resort, countermeasures are only supposed to be employed after submitting a formal request to the responsible state to remedy its internationally wrongful act (subject to certain exceptions).[78] A state may not employ countermeasures after an internationally wrongful act has ceased, and punitive countermeasures are prohibited.[79] Additionally, states use countermeasures at their own risk. Recall that countermeasures are otherwise-unlawful acts that are only permissible when used to induce another state's compliance with its international obligations. Should a state use countermeasures inappropriately or against the wrong entity, the original victim state becomes responsible for a new internationally wrongful act.[80]

These requirements severely hamper a state's ability to use countermeasures in response to cyberoperations. The speed and secrecy of cyber means that many harmful acts will have ended before they are discovered, let alone before the victim state is able to identify the responsible state and issue a request for cessation or employ a timely countermeasure. As there are myriad opportunities for victim states acting in good faith to misidentify perpetrators and for state and non-state actors to launch cyberoperations that encourage such misidentifications, states may be hesitant to employ countermeasures until they are reasonably certain of the perpetrator. Between uncertainty about what constitutes an internationally wrongful act and uncertainty about being able to make a reasonable attribution, states are likely to have delayed reactions to cyberoperations—and delayed reactions look more like prohibited punishment than permissible countermeasures.

Part of the problem is that countermeasures were never meant to be deterrents: at least theoretically, they are formally restricted to being used to restore the status quo prior to the perpetrator's legal violation.[81] In physical space, where many unlawful acts are public, relatively easily attributable, and take place over an extended period of time, the line between a victim state attempting to restore order and taking retaliatory action

---

respond with retorsions); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 714–30 (2014) (providing an in-depth analysis of the applicability of countermeasures to cyberoperations).

78 Draft Articles, *supra* note 47, arts. 43(2), 52(1).

79 *See id.* arts. 49(2), 50(1), 52(3).

80 *But see* TALLINN MANUAL 2.0, *supra* note 46, r. 20 cmt. 16 (noting a minority view that honest and reasonable mistakes are not unlawful).

81 *See* Draft Articles, *supra* note 47, ch. 2 cmt. 1.

was blurred, allowing lawful countermeasures to also serve as functional deterrents. This line is far crisper in cyberspace, rendering most countermeasures unlawful or of little use in addressing ongoing cyberoperations or deterring future ones.

Of course, states may always employ retorsions as a deterrent or punishment. Neither countermeasures nor retorsions need mirror the actions they are intended to stop or deter: a state victim to a harmful cyberoperation could respond with economic sanctions (as the United States did with North Korea following the Sony hack) or by ousting diplomats (as the United States did to Russian officials following the DNC hack). However, the possibility of unilateral retorsions does not appear to have been effective at deterring malicious cyberoperations.

3. *State Paralysis*

In the absence of clear rules delineating lawful and unlawful state behavior in cyberspace, victim states appear unsure of how to respond to harmful cyberoperations; even when they are reasonably certain of the perpetrator's identity, it is not clear what responsive measures they may take as a matter of law or should take as a matter of policy.[82]

At present, victim states seem to be erring on the side of minimal public action, possibly to avoid setting undesirable precedent or risking uncontrolled conflict escalation.[83] Consider the delayed U.S. reaction to the DNC hack. Although Russian involvement was suspected from the outset[84]—and, as has been subsequently disclosed, the United States had information that the Russian government had accessed the Democratic National Committee networks as early as July 2015[85]—the United States did not publicly attribute the hack to Russia

---

82 *See* Isabella Uría, *Hacking the Election Conference*, INFO. SOC'Y PROJECT & CTR. FOR GLOBAL LEGAL CHALLENGES (Sept. 20, 2016), http://isp.yale.edu/sites/default/files/hacking_the_election_conference_report_11.01.16_0.pdf [https://perma.cc/RN23-RLXX] (noting Susan Hennessey's description of states as being trapped in a "paralysis of too many options"). *But see* Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 TEX. L. REV. 1555, 1564 (2017) (suggesting that states' minimalist response to malicious cyberoperations is due more to uncertainty regarding attribution rather than uncertainty regarding the applicable law).

83 Uría, *supra* note 82 (noting Susan Hennessey's comment that the United States has "struggl[ed] to develop a comprehensive strategy for response to [cyberattacks]").

84 Hamburger & Tumulty, *supra* note 4.

85 David E. Sanger, *U.S. Reacting at Analog Pace to a Rising Digital Risk, Hacking Report Shows*, N.Y. TIMES (Jan. 7, 2017), https://www.nytimes.com/2017/01/07/us/politics/us-reacting-at-analog-pace-to-a-rising-digital-risk-hacking-report-shows.html?mcubz=0 [https://perma.cc/UPK4-NE5M].

until October 2016.[86] Then, after months of speculation and proposals as to what the United States might do in response,[87] the Obama Administration imposed sanctions on four individuals and five Russian entities, expelled thirty-five suspected Russian intelligence operatives, shut down two U.S.-based Russian compounds, and released information on Russian cybertactics and techniques.[88] Collectively, these actions constituted the strongest U.S. public response to a cyberoperation to date; nonetheless, they were widely derided as being insufficient to deter similar future cyberoperations.[89] Many are concerned that the U.S. "pattern of vacillation in response to very damaging cyber-operations will not deter our adversaries; it will embolden them."[90] Of course, the United States is not the only state victim to harmful cyberoperations; numerous other states have been subjected to similar actions (and the United States is recognized as a frequent perpetrator).[91] But this common minimalist response creates a permissive environment for state-sponsored cyberoperations.[92]

---

86 Sanger & Savage, *supra* note 6.

87 *See, e.g.*, James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POL'Y (Oct. 12, 2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/ [https://perma.cc/BPL2-2RZM] (outlining possible U.S. responses to the DNC hack, including "a definitive exposure of the Russian government's presumably high-level involvement in the attacks" with the hope of eventual U.N. condemnations and economic sanctions; "undermin[ing] the Russian government's reliance on a wide variety of cyber-tools to censor the web within its own country"; "expos[ing] the overseas banking accounts and financial resources of high-level Russian government officials"; "punish[ing] Russian hackers by knocking them off-line or even damaging their hardware"; or turning to allies for help).

88 Press Release, Office of the Press Sec'y, *supra* note 11.

89 *See, e.g.*, Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents*, LAWFARE (Jan. 9, 2017, 8:00 AM), https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents [https://perma.cc/H788-KGQ9] (providing examples).

90 Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE (Oct. 9, 2016, 6:27 PM), https://lawfareblog.com/dnc-hack-and-lack-deterrence [https://perma.cc/9FCP-QREW]. Representative Adam Schiff has suggested that the U.S. response to the Sony hack encouraged Russian hackers' interference in the 2016 U.S. election. Patricia Zengerle, *U.S. Lawmaker: Sony Breach May Have Inspired Russian Election Hacking*, REUTERS (Dec. 6, 2016, 3:41 PM), http://www.reuters.com/article/us-usa-cyber-russia-congress-idUSKBN13V2N3?il=0 [https://perma.cc/9YY5-6AS4].

91 *See, e.g.*, Desmond Butler, Jack Gillum & Alberto Arce, *U.S. Secretly Created 'Cuban Twitter' to Stir Unrest*, MIAMI HERALD (Apr. 3, 2014, 2:42 AM), http://www.miamiherald.com/news/nation-world/article1962295.html [https://perma.cc/7WHP-UUUB] (reporting on the U.S. attempt to destabilize the Cuban government through the creation of a Twitter-like social media platform).

92 Watts, *supra* note 20, at 250.

What is needed is a new deterrent, crafted in light of states' interest in exploring their expanded cyber-enabled capabilities and designed to address the harms caused by cyberoperations like the Sony and DNC hacks.[93] As discussed in the next section, holding states liable for their international cybertorts could be a solution to this problem.

II
STATE LIABILITY FOR INTERNATIONAL CYBERTORTS

An "international cybertort" is an act that employs, infects, or undermines the internet, a computer system, or a network and thereby causes significant transboundary harm.

Not only is it conceptually useful to differentiate international cybertorts from transnational cybercrime, cyberwarfare, and other kinds of cyberoperations, this term implies an alternative accountability mechanism and new deterrent for harmful state-sponsored cyberoperations: states could be required to compensate victims of their international cybertorts under the principle of state liability for transboundary harms.

A. A Distinct Kind of Harmful Cyberoperation

As mentioned in the Introduction, the North Korean "Guardians of Peace" hacker group raided Sony Entertainment Pictures servers and publicized extensive confidential data.[94] Based on an FBI analysis of the associated software, techniques, and network sources, the United States took the then-unprecedented move of publicly attributing the Guardians's cyberoperations to the state of North Korea.[95] Officially, the United States retorted by imposing new unilateral sanctions;[96] many suspect that it was also responsible for extensive North Korean web outages in early December 2014.[97] Meanwhile, as of February 2015, Sony estimated that its investigation and remediation costs had reached $15 million—ultimately, the total direct and indirect costs of the hack will likely be far greater, with some estimating that costs might include $80 million in direct damages and another $120 million in indirect damages

---

93 Crootof, *supra* note 89.

94 Robb, *supra* note 1.

95 Press Release, U.S. Dep't of Treasury, *supra* note 2; Nakashima, *supra* note 2.

96 Roberts, *supra* note 55.

97 *See* Strohm, *supra* note 11.

(such as leaked trade secrets and lost revenue).[98] How should the Sony hack be categorized?

To the extent it was conducted by or sponsored by a state, the Sony hack was not—or was not only—a transnational cybercrime.[99] A cybercrime occurs when a computer or program is used as the means to commit an illegal act.[100] Domestic cybercrimes are regulated internally; cross-border cybercrimes are investigated and prosecuted like other kinds of transnational crime. A paradigmatic example of transnational cybercrime occurred in August 2015, when Wall Street traders partnered with Ukrainian hackers to gain access to unpublished company press releases, allowing them to make trades that "reaped more than $100 million in illegal proceeds."[101] Significantly, only individuals are subject to criminal liability for cybercrimes—states cannot be held criminally liable, even for state-sponsored cybercrimes.[102] Thus, while the Guardians of Peace or identified state actors or agents could (theoretically) be criminally prosecuted for the Sony hack, the state of North Korea cannot.

Nor was the Sony hack an act of cyberwarfare. Although a cyberoperation might be intended to undermine a state's national security, be politically coercive, or cause extensive economic harm, such an action only constitutes cyberwarfare if it occurs in the context of an ongoing armed conflict or if it is sufficiently destructive in physical space to meet the "armed attack" threshold legitimizing defensive military action.[103]

Cyberoperations are increasingly being used in response to traditional provocations and in conjunction with more conven-

---

98 Brinded, *supra* note 3 (predicting that costs to Sony from hack would be $200 million); Cecilia Kang, *Sony Pictures Hack Cost the Movie Studio at Least $15 Million*, WASH. POST (Feb. 4, 2015), https://www.washingtonpost.com/news/business/wp/2015/02/04/sony-pictures-hack-cost-the-movie-studio-at-least-15-million/?utm_term=.db5b8a3b9915 [https://perma.cc/85JW-GXEL].

99 *See* Hathaway et al., *supra* note 77, at 830–31 (discussing why cybercrimes committed by non-state actors on behalf of a state raise international legal and national security issues that justify distinguishing them from other, less politically motivated, cybercrimes).

100 *See id.* at 833–34.

101 Matthew Goldstein & Alexandra Stevenson, *Nine Charged in Insider Trading Case Tied to Hackers*, N.Y. TIMES (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/business/dealbook/insider-trading-sec-hacking-case.html?_r=0 [https://perma.cc/BB6C-ZCEX].

102 Walton, *supra* note 17, at 1473–74.

103 Hathaway et al., *supra* note 77, at 821, 839–40 (concluding that "cyberwarfare" is "a term properly used only to refer to the small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict").

tional attacks in the context of ongoing armed conflicts. For example, the United States infiltrated the Iraqi Defense Ministry email system to inform Iraqi officers how they could peacefully surrender shortly before its 2003 invasion;[104] the Israeli Air Force used a cyberoperation to compromise the Syrian air-defense system during its 2007 air strike against a nuclear facility;[105] and, in the summer of 2008, Georgia's internet access was shut down while Russian forces invaded South Ossetia.[106] More recently, the United States has publicly announced that it is using cyberoperations in its campaign against the Islamic State, both to interfere with its communications strategy and to alter data in its systems.[107] "We are dropping cyberbombs," said then-Deputy Secretary of Defense Robert Work, "We have never done that before."[108] *Jus in bello* (the law governing the conduct of hostilities) regulates cyberoperations that occur in the context of an armed conflict[109]—but the Sony hack occurred during peacetime.

There is general agreement that *jus ad bellum* (the law governing the commencement of hostilities) regulates responses to cyberoperations that satisfy the armed attack threshold requirement,[110] and that a cyberoperation can meet that standard if its effects are equivalent to those of a conven-

---

104 RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 9–10 (2010).

105 Sharon Weinberger, *How Israel Spoofed Syria's Air Defense System*, WIRED (Oct. 4, 2007, 3:14 PM), https://www.wired.com/2007/10/how-israel-spoo/ [http://perma.cc/UR2G-PKZZ].

106 Travis Wentworth, *How Russia May Have Attacked Georgia's Internet*, NEWSWEEK (Aug. 22, 2008, 8:00 PM), http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111 [https://perma.cc/4SVD-8MZH]. It is unclear if the Russian government planned the incident or stood by while private hackers openly celebrated the attack. Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST: SECURITY FIX (Oct. 16, 2008, 3:15 PM), http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html [https://perma.cc/9G6W-YKZB]; Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009, 12:45 PM), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ [https://perma.cc/9QJR-A56A].

107 David E. Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N.Y. TIMES (Apr. 24, 2016), http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html [https://perma.cc/3EBX-XV4B].

108 *Id.*

109 TALLINN MANUAL 2.0, *supra* note 46, r. 80.

110 *See, e.g.*, *id.* r. 71. *But see id.* ch. 14 cmt. 3 (noting that the *Tallinn Manual 2.0* applies the *lex lata* norms in the cyber context, but that these are subject to change based on state practice).

tional armed attack.[111] However, the vast majority of harmful cyberoperations cause non-physical damage that simply does not register on the cyberwarfare spectrum. Notwithstanding perennial academic interest in the question, at present only one cyberoperation—the 2010 Stuxnet attack—has arguably had sufficiently destructive effects to meet the armed attack threshold.[112] The Stuxnet attack, which destroyed 1,000 Iranian centrifuges used to enrich uranium, was the first time computer malware was recognized as capable of specifically targeting and destroying industrial systems.[113] Despite the military nature of the target and the extent of the damage, experts continue to disagree as to whether even Stuxnet qualified as an armed attack.[114] With no military nexus and no loss of life, the Sony hack does not come close to meeting the armed attack threshold.

---

111 *Id.* r. 69 cmts. 8–11; Hathaway et al., *supra* note 77, at 836–37. Notably, in 2014 NATO declared that it would consider a cyberoperation that rose to the level of an armed attack on one of its member states to trigger the collective defense requirement expressed in Article 5 of the North Atlantic Treaty. Andrea Shalal, *Massive Cyber Attack Could Trigger NATO Response: Stoltenberg*, REUTERS (June 15, 2016, 5:38 PM), https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE [https://perma.cc/9Y4V-UZ4M]. NATO's Secretary General reiterated this statement in response to the June 2017 NotPetya malware attacks. *NotPetya Joint Response*, *supra* note 70.

112 TALLINN MANUAL 2.0, *supra* note 46, at r. 71 cmt. 10. To date, only a handful of cyberoperations are known to have caused physical damage. These include the 2010 Stuxnet malware that destroyed Iranian centrifuges, Kelley, *supra* note 31; the 2012 attack on the Saudi Arabian oil company, Aramco, which destroyed 30,000 computers, Daniel Fineren & Amena Bakr, *Saudi Aramco Says Most Damage from Computer Attack Fixed*, REUTERS (Aug. 26, 2012, 2:55 PM), http://www.reuters.com/article/net-us-saudi-aramco-hacking/saudi-aramco-says-most-damage-from-computer-attack-fixed-idUSBRE87P0B020120826 [https://perma.cc/3LXA-FYRW]; the 2014 hack and destruction of a German steel mill, Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, WIRED (Jan. 8, 2015, 5:30 AM), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [https://perma.cc/U8SW-EMZ6]; the destruction of 3,000 computers and 800 servers during the 2014 Sony hack, Steve Kroft, *The Attack on Sony*, CBS NEWS (Apr. 12, 2015), https://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/ [https://perma.cc/UE67-R8S8]; the 2015 attacks that shut down the Ukrainian power grid, Zetter, *supra* note 33; and possibly the 2008 explosion of a Turkish oil pipeline, Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG (Dec. 10, 2014, 5:00 AM), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar [https://perma.cc/YTK4-38S3].

113 *See* Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets,'* BBC NEWS (Sept. 23, 2010), http://www.bbc.co.uk/news/technology-11388018 [https://perma.cc/KJ6B-PVBE].

114 TALLINN MANUAL 2.0, *supra* note 46, r. 71 cmt. 10.

So what was the Sony hack? Prominent writers refer to it as a "below the threshold" cyberoperation[115] or a "low-intensity cyber operation[ ]," defined as an "action[ ] taken short of [a] destructive or violent attack[ ]."[116] Such characterizations imply that these cyberoperations exist in the negative space surrounding the law of armed conflict, and in doing so fail to recognize them as a distinct kind of cyberincident with a different primary harm.[117] In acknowledgement of the significant injuries associated with cyberoperations like the Sony hack, this Article suggests switching legal frameworks entirely—to tort law.

B. International Cybertorts

The Sony hack is best understood as an international cybertort. As opposed to the law of war, which rarely addresses the impact of low-level physical damage, economic harms, or reputational costs; or criminal law, which is designed to hold individuals accountable for their morally blameworthy wrongs, tort law allocates liability for intended and unintended injuries. Recognizing international cybertorts as a distinct category allows for a more accurate assessment of the harms associated with different cyberoperations, and by extension, a more considered discussion of how to construct appropriate accountability regimes for state action in cyberspace.[118]

Again, an "international cybertort" is an act that employs, infects, or undermines the internet, a computer system, or a network and thereby causes significant transboundary harm. Like the definition of transnational cybercrime, the international cybertort definition is means-based and encompasses a broad range of harmful activities.[119] Rather than focusing on the intent of the actor—always a thorny question in contexts

---

115 Schmitt, *supra* note 77, at 698.

116 Watts, *supra* note 20, at 250.

117 The Sony hack's relationship with cyberespionage, sovereignty violations, interference, and intervention is discussed below. *See infra* section II.B.1.

118 In contrast, domestic cybertorts—which often are alleged in any situation where the internet or a computer system is used to commit a civil wrong—are grounded in and therefore limited by domestic tort law, which usually grants immunity to sovereign states. *See* Daniel Blumenthal, *How to Win a Cyberwar with China*, FOREIGN POL'Y (Feb. 28, 2013), http://foreignpolicy.com/2013/02/28/how-to-win-a-cyberwar-with-china-2/ [https://perma.cc/54K6-PABN].

119 Unlike the definition of a cybercrime, the definition of cyberwarfare is objective-based. *See* Hathaway et al., *supra* note 77, at 826–28.

where states are legal actors[120]—this definition depends on the effects of the action. In encompassing both intended and unintended harms, it implicitly takes the position that the injury sustained by the victim is of more import than the intention of the cybertortfeasor.

Importantly, the original state conduct need not itself be unlawful—rather, it is the resulting harm that raises the possibility of tort liability. This is often the case in domestic law: driving an automobile or using dynamite are lawful, albeit regulated, activities—when their use causes harm, however, the user may be liable in tort. As a result, this definition covers far more activities than would be addressed under the law of state responsibility.

1. *Relationship with Cybercrime and Cyberwarfare*

In many domestic legal systems, the same action may sometimes be both a crime and a tort: similarly, an international cybertort may sometimes also be a transnational cybercrime or, if the harm is sufficiently destructive, cyberwarfare. For example, the Stuxnet attack destroyed at least one thousand Iranian centrifuges.[121] Assuming Iran was interested in pressing the issue, it has a credible case that this harm constituted an international cybertort. If Stuxnet was the work of non-state actors, it might also be a transnational cybercrime; if it can be sufficiently attributed to a state, it could arguably be considered cyberwarfare.

Figure 1 summarizes the similarities and distinctions between these different kinds of cyberoperations; Figure 2 illustrates the relationships between international cybertorts, transnational cybercrimes, and cyberwarfare, emphasizing that these categories are not mutually exclusive. It locates the Sony hack on the intersection of cybercrime and international cybertorts to encompass both the criminal liability of the individual hackers who engaged in the attack and the liability of the state that allegedly sponsored the attack.

---

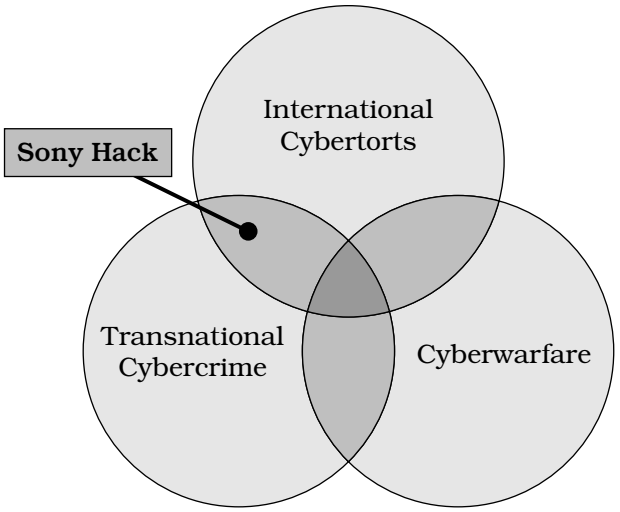
120 *Cf.* Rebecca Crootof, *Change Without Consent: How Customary International Law Modifies Treaties*, 41 YALE J. INT'L L. 237, 254–56 (2016) (discussing difficulties associated with identifying state intent when interpreting treaties).

121 Joseph Menn, *Exclusive: U.S. Tried Stuxnet-Style Campaign Against North Korea but Failed – Sources*, REUTERS (May 29, 2015, 3:01 PM), http://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529 [https://perma.cc/8XME-C2Q3].

FIG. 1: TYPES OF CYBEROPERATIONS

	International Cybertort	**Transnational Cybercrime**	**Cyberwarfare**
Distinguishing Characteristics	The original cyberoperation need not be unlawful, but the act must cause significant transboundary harm.	Must be a violation of criminal law and committed by means of a computer system.	Must have a political or national security purpose and either (1) be sufficiently destructive to satisfy the "armed attack" threshold; or (2) occur in the context of an armed conflict.
Governing Legal Regime	State Liability for Transboundary Harm[122]	Domestic and International Criminal Law	(1) *Jus ad Bellum*; and (2) *Jus in Bello* (International Humanitarian Law)
Paradigmatic Example	Sony Hack	Ukrainian Hacker Insider Trading Ring	(1) Possibly Stuxnet; (2) U.S. cyberoperations against the Islamic State

FIG. 2: RELATIONSHIPS AMONG THE CATEGORIES[123]



122 *See infra* subpart II.C.

123 Figure 2 is intended to clarify the relationship among the different labels for different kinds of cyberoperations; it is not meant to represent the proportions of different types of cyberoperations.

2. *Relationship with Data Destruction and Ransomware*

Recognizing international cybertorts as a distinct category suggests a solution for a question currently vexing cyberwarfare scholars: how to classify cyberoperations that affect access to data, either by destroying it or by holding it hostage. These attacks have myriad costly, chaotic, and even deadly effects, limited only by one's imagination. Academic medical research centers or pharmaceutical companies could have years of trials wiped out; registered voters could be removed from the rolls; a lifetime's worth of credit-building could disappear overnight; selective deletions of flight plans could lead to in-air collisions; the entire stock market could be thrown into chaos; information on life-threatening allergies could be removed from medical records.

Thus far, data-destruction cyberincidents have not caused any physical effects on these scales, but they have demonstrated the potential scope of the risk. In 2011, "half of the 500-plus servers belonging to [South Korea's Nonghyup Bank] were crippled [by a data-destruction attack], including servers controlling ATMs, credit card access, and online banking."[124] This affected approximately 30 million customers, leading to "more than 30,000 customer complaints and 1,000 compensation claims."[125] More recently, the June 2017 NotPetya malware—so named because it presents as Petya ransomware, though it appears only capable of rendering data completely inaccessible—spread across the globe.[126] During this attack, ATMs stopped working, banks were forced to close, hospitals canceled operations, and the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline.[127]

Ransomware attacks can be just as devastating. Ransomware infiltrates network systems, encrypts vital files and

---

124 FED. BUREAU OF INVESTIGATION, INTELLIGENCE ASSESSMENT: POTENTIAL IMPACTS OF A DATA-DESTRUCTION MALWARE ATTACK ON A US CRITICAL INFRASTRUCTURE COMPANY'S NETWORKS (2013), at 7, https://firstlook.org/wp-uploads/sites/1/2014/12/2013-FBI-REPORT-2.pdf [https://perma.cc/T2NV-N5CU].

125 *Id.*

126 Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine then Spreads Internationally*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?mcubz=0&_r=0 [http://perma.cc/34F5-QCKV]; *see also* Iain Thomson, *Everything You Need to Know About the Petya, er, NotPetya Nasty Trashing PCs Worldwide*, REGISTER (June 28, 2017, 3:19 AM), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/ [https://perma.cc/QX9E-7X4H] (describing NotPetya and linking it to the June 2017 cyberattacks that shut down Chernobyl's monitoring systems).

127 Perlroth et al., *supra* note 126.

data, and demands payment in return for the key to unlocking the information.[128] The data in question is never destroyed, but it is rendered effectively nonexistent. Hospitals' patient data is often targeted, as are companies' files with their customers' credit card data.[129] A cybersecurity expert estimated that cybercriminals made over $1 billion in 2016 alone from ransomware.[130] In early 2017, in the largest ransomware assault to date,[131] a variant of the WannaCry ransomware "crippled 200,000 computers in more than 150 countries."[132] It "forc[ed] Britain's public health system to send patients away, [froze] computers at Russia's Interior Ministry and [wreaked] havoc on tens of thousands of computers elsewhere."[133]

A cyberoperation that compromises hospital records, banking data, or trade secrets is not an act of war,[134] but it also

---

128 Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, WIRED (May 14, 2017, 1:00 PM), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ [https://perma.cc/8PSR-YEDF].

129 *See, e.g.*, Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016, 10:44 AM), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html [http://perma.cc/YCM7-V3LF].

130 Maria Korolov, *Ransomware Took in $1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide*, CSO (Jan. 5, 2017, 4:25 AM), http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html [http://perma.cc/9R75-JC9L].

131 Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?mcubz=0 [https://perma.cc/FY4W-ZC77].

132 Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?mcubz=0 [https://perma.cc/XU5L-83PX].

133 Perlroth & Sanger, *supra* note 131.

134 To the extent international cybertorts might apply to actions taken in the context of an armed conflict, they also might help address a long-standing debate about whether or not data is a lawful target. International humanitarian law prohibits attacks on civilian objects, and the *Tallinn Manual 2.0* extends this prohibition to cyber infrastructure. TALLINN MANUAL 2.0, *supra* note 46, r. 99 ("Civilian objects shall not be made the object of cyber attacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective."). However, the majority of the *Tallinn Manual 2.0* experts determined that "the law of armed conflict notion of 'object' is not to be interpreted as including data." *Id.* r. 100 cmt. 6. They reasoned that "data is intangible and therefore neither falls within the 'ordinary meaning' of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary." *Id.* (footnote omitted). In other words, data may sometimes be a lawful target. A minority disagreed, contending that "for the purposes of targeting, certain data should be regarded as an object." *Id.* at r. 100 cmt. 7. Were that not the case, they argued, the deletion of even "essential civilian datasets such as social security data, tax

cannot be tolerated. The concept of international cybertorts provides a means of holding states accountable for their data destruction and ransomware attacks.

3. *Relationship with Cyber Exploitation and Cyberespionage*

Cyber exploitation is the act of gathering confidential information kept on or transiting through a computer system or network, usually secretly and often for commercial purposes; cyberespionage is cyber exploitation conducted for political or military purposes.[135] An act may be simultaneously cyber exploitation or cyberespionage and an international cybertort, but only if the act is detected or publicized (as discovery of the intrusion will usually require extensive remediation).

There are numerous examples of cyber exploitation, some of which might also constitute cyberespionage. In 2014, hackers believed to be working for the Russian government breached the White House's unclassified network, gaining access to President Obama's schedule and emails and, by extension, information regarding personnel moves and policy

---

records, and bank accounts would potentially escape the regulatory reach of the law of armed conflict." *Id.* According to the minority, this would "run[ ] counter to principle (reflected in Article 48 of Additional Protocol I) that the civilian population enjoys general protection from the effects of hostilities." *Id.* While I agree with the minority, introducing the concept of international cybertorts helps alleviate the injuries that would likely accompany the majority's approach: regardless of whether or not data is a lawful target, states might be held liable for its destruction.

I have argued elsewhere that states should be held strictly liable for the actions taken by their autonomous weapon systems. *See* Crootof, *War Torts*, *supra* note 19, at 1394–96. Some aspects of this argument might be extrapolated to all accidents that occur in the context of an armed conflict.

135 *See* Hathaway et al., *supra* note 77, at 829 n.48. There is no widely-accepted definition of either of these terms. My definitions are intended to convey that actions constituting cyber exploitation may be directed against state or non-state actors by state or non-state actors; consist of gathering information on a computer system or network; are not primarily intended to cause death, injury, destruction, or damage; are usually (though not necessarily) conducted secretly; and often involve gathering information for commercial purposes. Other definitions focus on different aspects: sometimes on the parties involved, sometimes on the means of conducting the attack, and sometimes on the objectives of the attack. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 46, r. 32 cmt. 2 (defining peacetime cyberespionage as "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information"); Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War?*, NEW YORKER (Nov. 1, 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh? [http://perma.cc/Y72J-8VJY] (defining cyberespionage as "the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence").

debates.[136] Also in 2014, what was likely the same group hacked into the Department of State's unclassified email network, prompting a complete system shutdown.[137] In 2015, Chinese hackers broke into the U.S. Office of Personnel Management (OPM) database and made off with the personal information of more than 22 million individuals who had undergone federal security screenings, including 4.2 million federal employees.[138] These same hackers are likely also responsible for the February 2015 hack of Anthem, Inc., which compromised the personal information of roughly 80 million current and former customers, and the July and August 2015 hacks of United Airlines and American Airlines.[139]

The 2016 DNC hack was a more complicated combination of cyberespionage and information warfare. In June 2016, the Democratic National Committee hired Crowdstrike to investigate a detected hack. Crowdstrike determined that the DNC had been subject to two distinct hacks, conducted by groups nicknamed Cozy Bear and Fancy Bear and associated with two organizations in the Russian government.[140] Over 19,000 emails obtained through these hacks were then released, presumably with the intent of sowing confusion in the Democratic party.[141]

If the injuries associated with these cyber exploitation and cyberespionage operations are sufficiently significant, they could be considered international cybertorts. And there is evidence that the harms are immense. With the exception of the

---

136 Paul Szoldra, *The 9 Worst Cyberattacks of 2015*, BUS. INSIDER (Dec. 30, 2015, 9:10 AM), http://www.techinsider.io/cyberattacks-2015-12 [http://perma.cc/J5BR-22RG].

137 Evan Perez & Shimon Prokupecz, *Sources: State Dept. Hack the 'Worst Ever,'* CNN (Mar. 10, 2015, 7:49 PM), http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html [http://perma.cc/EEW4-6JUV].

138 Szoldra, *supra* note 136. The Chinese government has asserted that the OPM hack was criminal activity rather than a state-sponsored cyberoperation. Michael Forsythe & David E. Sanger, *China Calls Hacking of U.S. Workers' Data a Crime, Not a State Act*, N.Y. TIMES (Dec. 2, 2015), https://www.nytimes.com/2015/12/03/world/asia/china-hacking-us-opm.html?mcubz=0 [https://perma.cc/GQE8-PGVG].

139 Riley Walters, *Cyber Attacks on U.S. Companies Since November 2014*, HERITAGE FOUND. (Nov. 18, 2015), http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014 [https://perma.cc/B5ME-792M].

140 Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST (June 20, 2016), https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html?utm_term=.35db1c96547a [https://perma.cc/SPM2-KEQU].

141 Hamburger & Tumulty, *supra* note 4.

DNC hack, these cyberoperations were likely intended to be covert—but once discovered, the hacked entities had to spend huge sums to expunge hackers, compensate customers, and rebuild reputations. Costs differ by industry: the average hack of hospital records can range from a few hundred thousand to three million dollars,[142] while the total costs of a retailer data breach might range from two to six million dollars.[143] The costs of government hacks are harder to calculate—but there are estimates that the OPM hack alone is costing taxpayers $350 million.[144] Given that there are roughly 35,000 known computer security penetration incidents per day, the collective costs are staggering.[145] A 2014 study estimated that cyberoperations cost businesses between $375 and $575 billion annually;[146] a 2016 analysis suggests that costs will reach $6 trillion annually by 2021.[147]

Distinguishing international cybertorts from transnational cybercrimes and cyberwarfare promotes a more precise understanding of the distinct kinds of harms associated with these different cyberoperations. As discussed in the next section, this new terminology also highlights the possibility of an alternative means of holding states accountable for their harmful cyberoperations, thereby creating a new, less-escalatory responsive option for victim states.

C. State Liability

The principle of state liability for transboundary harms holds states accountable for the "injurious consequences that arise out of activities within their jurisdiction or control and that affect other States or nationals of other States."[148]

Conceptually, this principle—that states should be held accountable for the harm they cause—already undergirds the

---

142 Rosalie L. Donlon, *Hacked! The Cost of a Cyber Breach, in 5 Different Industries*, PROPERTYCASUALTY360 (Oct. 16, 2015), http://www.propertycasualty360.com/2015/10/16/hacked-the-cost-of-a-cyber-breach-in-5-different-i [http://perma.cc/UV9Y-BQ47].

143 *Id.*

144 Elizabeth Harrington, *OPM Hack Costing Taxpayers $350 Million*, WASH. FREE BEACON (Sept. 2, 2015, 10:39 AM), http://freebeacon.com/issues/opm-hack-costing-taxpayers-350-million/ [http://perma.cc/CJZ2-MVLT].

145 Donlon, *supra* note 142.

146 CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [http://perma.cc/A59Y-S5X6].

147 CYBERSECURITY VENTURES, *supra* note 16.

148 Sompong Sucharitkul, *State Responsibility and International Liability Under International Law*, 18 LOY. L.A. INT'L & COMP. L.J. 821, 822 (1996).

law of state responsibility, which requires states to make appropriate reparations for their internationally wrongful acts.[149] As a result, state liability and state responsibility are often conflated.[150] However, the law of state responsibility does not address harmful state operations that are not also wrongful or attributable.[151] Given the differing harms state liability and state responsibility are meant to correct, their approaches and consequences differ: state liability is primarily concerned with ensuring compensation for injuries,[152] while state responsibility aims to restore the status quo prior to an internationally wrongful act through a broader range of restitutive means.[153] State liability should therefore be recognized as an independent principle, applicable in situations where there is no act or omission that violates a state's international obligations.[154] Once distinguished from state responsibility and its requirement of an internationally wrongful act, the principle of state liability for transboundary harms creates new responsive options for states experiencing the harmful transboundary consequences of another state's activities.

1. *State Liability for Transboundary Harms*

The intuitive idea that one is liable for caused harm is well-established in international law. It is articulated in the Roman maxim *sic utere tuo ut alienum non laedas*[155] and in Grotius's statement that from any "Fault or Trespass there arises an

---

149 *See infra* section III.A.3.

150 Indeed, some have suggested that the movement to distinguish the doctrine of state liability for transboundary harms is "fundamentally misconceived." Alan E. Boyle, *State Responsibility and International Liability for Injurious Consequences of Acts Not Prohibited by International Law: A Necessary Distinction?*, 39 INT'L & COMP. L.Q. 1, 13 (1990) (quoting IAN BROWNLIE, STATE RESPONSIBILITY: PART I 50 (1983)).

151 This gap is what originally spurred the General Assembly to task the International Law Commission with evaluating the subject of state liability for transboundary harms. G.A. Res. 32/151, ¶ 7 (Dec. 19, 1977) [hereinafter ILC Report].

152 Pemmaraju Sreenivasa Rao (Special Rapporteur), *Third Rep. on International Liability for Injurious Consequences Arising out of Acts Not Prohibited by International Law (Prevention of Transboundary Damage from Hazardous Activities)*, U.N. Doc. A/CN.4/510 (June 9, 2000), at 121 ("[W]rongful acts are the focus of State responsibility, whereas compensation for damage [is] the focus of international liability.").

153 *See infra* section III.A.3.

154 *See* Boyle, *supra* note 150, at 3 ("What distinguishes international liability from other forms of responsibility is that it does not presuppose wrongful conduct or breach of any obligation.").

155 "Use your own property in such a way that you do not injure other people's." *Sic Utere Tuo Ut Alienum Non Laedas*, OXFORD REFERENCE, http://www.oxfordreference.com/view/10.1093/oi/authority.20110803100504563 [https://perma.cc/Y2XD-7TCE].

Obligation by the Law of Nature to make Reparation for the Damage, if any be done."[156] Today, the concept that one may be liable for caused harms is common to many domestic legal systems[157] and reiterated in case law, treaties, and International Law Commission (ILC) reports and draft articles.

For nearly seventy years, various kinds of state liability for transboundary harms have been recognized in international jurisprudence.[158] In the 1941 *Trail Smelter* arbitration, in which the United States claimed damages resulting from a Canadian smelter's actions,[159] the tribunal proclaimed 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."[160] Shortly thereafter, the International Court of Justice (ICJ) echoed the *Trail Smelter* language in its *Corfu Channel* decision. After holding that Albania was under an obligation to warn other states that the Corfu Channel—a normally safe strait often used for international navigation—was mined, the Court stated that this obligation sprang from general international law:

> The obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them. Such obligations are based, not on the Hague Convention of 1907, No. VIII, which is applicable in time of war, but on certain general and well-recognized principles, namely: *elementary considerations of humanity, even more exacting in peace than in war*; the principle of the freedom of maritime communication; and *every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*.[161]

---

156 HUGO GROTIUS, 2 THE RIGHTS OF WAR AND PEACE 884, ¶ I (Richard Tuck ed., Jean Barbeyrac trans., 2005) (1625); *see also* Walton, *supra* note 17, at 1480 (discussing how, in Grotius's time, the failure to provide compensation could itself be a just cause for war).

157 *See, e.g.*, Int'l Law Comm'n, Survey of Liability Regimes Relevant to the Topic of International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law (International Liability in Case of Loss from Transboundary Harm Arising Out of Hazardous Activities), U.N. Doc. A/CN.4/543 (June 24, 2004), at ¶ 112 (noting that "strict liability, as a legal concept, now appears to have been accepted by most legal systems," though "[t]he extent of activities subject to strict liability may differ").

158 *See* Walton, *supra* note 17, at 1478–84 (discussing relevant case law).

159 *Id.* at 1479.

160 Trail Smelter (U.S. v. Can.), Award, 3 R.I.A.A. 1905, 1965 (Mar. 11, 1941).

161 Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9) (emphasis added).

States have regularly concluded treaties creating or clarifying liability for specific acts or omissions.[162] While drafted over many decades, these treaties generally focus on a few, specific kinds of harms (injuries associated with nuclear accidents, oil spills, and other kinds of hazardous materials) or harms which endanger the use of shared spaces (international watercourses, transboundary waters, and outer space). The strongest statement of state liability is found in the 1972 Convention on the International Liability for Damage Caused by Space Objects.[163] It provides that "[a] launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight,"[164] and includes more complicated standards—including joint and several liability and a contributory negligence defense—for non-Earth damage.[165]

In 1978, the U.N. General Assembly charged the ILC "to commence work on the topics of international liability for injurious consequences arising out of acts not prohibited by international law and jurisdictional immunities of States and their

---

162 These include the 1960 Paris Convention on Third Party Liability in the Field of Nuclear Energy; the 1962 Convention on the Liability of Operators of Nuclear Ships; the 1963 Vienna Convention on Civil Liability for Nuclear Damage; the 1969 International Convention on Civil Liability for Oil Pollution Damage; the 1972 Convention on International Liability for Damage Caused by Space Objects; the 1977 International Convention on Civil Liability for Oil Pollution Damage resulting from the Exploration for and Exploitation of Seabed Mineral Resources; the 1989 Convention on Civil Liability for Damage Caused during Carriage of Dangerous Goods by Road, Rail, and Inland Navigation Vessels; the 1989 Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal; the 1992 Convention on the Protection of the Marine Environment of the Baltic Sea Area; the 1992 Convention on the Transboundary Effects of Industrial Accidents; the 1992 International Convention on Civil Liability for Oil Pollution Damage; the 1993 Convention on Civil Liability for Damage Resulting from Activities Dangerous to the Environment; the 1996 International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea; the 1997 Convention on the Law of Non-Navigational Uses of International Watercourses; the 1997 Convention on Supplementary Compensation for Nuclear Damage; the 1999 Basel Protocol on Liability and Compensation for Damage Resulting from Transboundary Movements of Hazardous Wastes and their Disposal (not in force); the 2001 International Convention on Civil Liability for Bunker Oil Pollution Damage; and the 2003 Protocol on Civil Liability and Compensation for Damage Caused by the Transboundary Effects of Industrial Accidents on Transboundary Waters.

163 Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187.

164 *Id.* art. II. This absolute liability is subject to a defense that the damage resulted "wholly or partially from gross negligence or from an act or omission done with intent to cause damage on the part of a claimant State or of natural or juridical persons it represents." *Id.* art. VI.

165 *Id.* arts. III, IV, V, XXII.

property."[166] This project, originally an attempt "to conceptualize and circumscribe" state liability generally,[167] was later limited to environmental matters because of a lack of consistent state practice in other areas.[168] The ILC produced two circumscribed documents: the 2001 draft articles on the duty to prevent transboundary harm from hazardous activities and the 2006 draft principles regarding liability for the injurious consequences of such actions.[169] One particularly interesting conclusion of the ILC process was a clarification of the relationship between the principle of state liability and the law of state responsibility. When a state engages in an act that is not inherently unlawful but nonetheless causes harm—say, engaging in cyberespionage—the failure to provide compensation for the harm might itself constitute an internationally wrongful act, triggering the applicability of the law of state responsibility and its broader remedial measures.

Today, the principle of state liability is primarily discussed in terms of international environmental law, largely because of the paucity of situations outside of the environmental context where state action causes significant transboundary harm. But while the doctrine of state liability for transboundary harms has been most developed in environmental law, it is

---

166 ILC Report, *supra* note 151, ¶ 7.

167 Sucharitkul, *supra* note 148, at 829.

168 *See* Robert Q. Quentin-Baxter (Special Rapporteur), *Fourth Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, ¶ 15, U.N. Doc. A/CN.4/373 (June 27, 1983) ("[T]here is no possibility of proceeding inductively from the evidence of State practice in the field of the physical uses of territory to the formulation of rules or guidelines in the economic field.").

Critics had two main complaints regarding the ILC's project: first, they argued that there was no conceptual need to distinguish state liability from state responsibility; second, they claimed that the distinction would be of little use in developing international environmental law—and might even undermine other nascent environmental legal protections. Boyle, *supra* note 150, at 1.

169 For the 2001 draft articles, see Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 148 (2001). For the 2006 draft principles, see Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising Out of Hazardous Activities, with Commentaries, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Eighth Session, U.N. Doc. A/61/10, at 110 (2006) [hereinafter Draft Principles on the Allocation of Loss]. The former concerned states' obligations to avoid and minimize transboundary harm. The latter focused on operator liability, primarily because state liability was considered to be the exception in the treaty law. Apart from the Outer Space Treaty, most treaty regimes assigned liability for transboundary harms to non-state entities. *See, e.g.*, International Convention on Civil Liability for Oil Pollution Damage art. III, Nov. 29, 1969, 973 U.N.T.S. 3 (imposing liability on owners of ships that cause oil pollution, instead of on the ship owners' states).

hardly conceptually limited to that legal regime.[170] In the *Corfu Channel* case, the ICJ was not overly concerned with the environmental impact of the mines. Instead, the case was primarily about the use of military weapons in peacetime and the creation of a hazard in an otherwise safe passage used by other states.[171] The advent of increasingly harmful state-sponsored cyberoperations and lack of effective deterrents highlights a need for a new regulatory regime—and the principle of state liability for transboundary harms provides a useful framework for thinking about state accountability in this context.[172]

2. *Benefits of State Liability for International Cybertorts*

There are a number of benefits that would attend applying the principle of state liability to cyberoperations that cause significant transboundary harm. Holding states liable for the harmful consequences of their cyberoperations imposes costs on such activity, creating a new deterrent and increasing the likelihood that victims of international cybertorts will be compensated for their injuries. Simultaneously, labeling a harmful cyberoperation an international cybertort does not mean that it was necessarily unlawful, creating an intermediate space between cyberwarfare and unproblematic state activity in cyberspace.

a. *Creates a Non-Escalatory Responsive Option and New Deterrent*

At the time, President Obama described the Sony hack as "cybervandalism"—and was slammed domestically for what was perceived as a weak characterization.[173] But what was he to call it? Calling it cyberwarfare, as some would have preferred, would have stretched the definition of cyberwarfare beyond recognition and would set a precedent for other states to term similar U.S. cyberoperations cyberwarfare—and possibly take responsive action.

Still, "cybervandalism" clearly is not the right term. It usually describes the annoying but relatively innocuous practice of altering online content, like website defacement. In 2010, for example, photos of Spanish Prime Minister Jose Luis Rodri-

---

170 Walton, *supra* note 17, at 1480.
171 *See id.* at 1483–84.
172 *See id.* at 1511–19.
173 Brian Fung, *Obama Called the Sony Hack an Act of 'Cyber Vandalism.' He's Right.*, WASH. POST (Dec. 22, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/22/obama-called-the-sony-hack-an-act-of-cyber-vandalism-hes-right/?utm_term=.c9e20c2fcedb [https://perma.cc/B5E2-Z9KE].

guez Zapatero on a European Union website were replaced with a close-up shot of Mr. Bean.[174] "Cybervandalism" hardly seems to encompass the physical damage, economic costs, and reputational harms associated with the Sony hack. The language of tort law—and the term "international cybertorts"—does.

The possibility of labeling a cyberoperation an international cybertort and calling for compensation creates a new responsive option for a victim state, minimizing the likelihood that it will resort to more escalatory self-help options. Furthermore, the possibility of liability might operate as a new ex ante deterrent by imposing additional costs on engaging in cyberoperations that risk causing significant transboundary harm.

b. *Encourages Victim Compensation*

The principle of state liability for transboundary harms can be employed to increase the likelihood that states or their nationals will be compensated for their injuries. Different treaty regimes have developed different means by which harmed entities may bring claims for compensation: sometimes private entities bring claims against private entities, sometimes private entities bring claims against states, sometimes states bring claims against private entities, and sometimes states bring claims against states. These various approaches have corresponding benefits and drawbacks, and a careful analysis of the architecture of cyberspace and what practices have been effective in similar existing regimes is needed to determine what compensation structure will be preferable in the cyber context.

With regard to the Sony hack, the U.S. National Security Council Spokesman has already suggested that North Korea is liable for the millions in losses Sony suffered.[175] However, North Korea is unlikely to pay such compensation. This is not a damning indictment of the concept of international cybertorts, however, nor a unique phenomenon; domestic tort law plaintiffs are often unable to recoup their losses from judg-

---

174 *Mr Bean Replaces Spanish PM on EU Presidency Site*, BBC NEWS (Jan. 4, 2010), http://news.bbc.co.uk/2/hi/8440554.stm [https://perma.cc/B462-L9WX].

175 Julie Makinen, *North Korea Decries U.S. Allegations on Sony Hack; U.S. Turns to China*, L.A. TIMES (Dec. 20, 2014, 3:34 PM), http://www.latimes.com/world/asia/la-fg-north-korea-proposes-joint-investigation-into-sony-hack-20141220-story.html [https://perma.cc/S3SC-WLQP] ("[W]e are confident the North Korean government is responsible for this destructive attack . . . . If [they want] to help, they can admit their culpability and compensate Sony for the damages this attack caused.").

ment-proof defendants. While it may be sometimes impossible to compensate the victims of international cybertorts—either because there is no procedure in place for doing so, or because the perpetrator is already a rogue state and relatively immune to the threat of outcasting[176]—identifying international cybertorts still allows victim states to name the action and shame the liable state for not providing appropriate compensation.

c. *Creates a Bounded Grey Zone for State Experimentation in Cyberspace (And a New Means for Managing Cyberespionage)*

Perhaps President Obama used the term cybervandalism in describing the Sony hack to avoid raising the question of the lawfulness of U.S. cyberoperations, or perhaps he used it because there was no accurate term that allowed him to denounce the Sony hack without implying the appropriateness of a military response to the hack of a civilian business.[177] The concept of international cybertorts walks this thin line. Because the activity underlying an international cybertort is not necessarily unlawful, the term allows states suffering from an act's consequences to claim compensation without prejudging its lawfulness. The concept of international cybertorts thereby creates an intermediate space between unproblematic state activity in cyberspace and cyberwarfare, preserving a bounded grey zone for state experimentation.

The possibility of managing cyberoperations in this intermediate space has considerable implications for cyberespionage. Thus far, governments have had few means of deterring cyber exploitation and cyberespionage. There is little law on the subject: the United States, one of the loudest critics of cyber-enabled industrial espionage, nonetheless maintains that "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. . . . This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects."[178]

---

176 *See* Oona Hathaway & Scott J. Shapiro, *Outcasting: Enforcement in Domestic and International Law*, 121 YALE L.J. 252, 340 (2011) (pointing out that outcasting regimes have little enforcement power over isolated states).

177 Fung, *supra* note 173 ("What's really going on here is a battle to determine whether, in fact, the infiltration of corporate networks, exposure of business information and censorship of U.S. film studios is a legitimate military activity.").

178 Brian J. Egan, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016), https://www.law.berkeley.edu/wp-con

While states are not held formally accountable for their spies' actions in the physical world, individual spies could be apprehended, prosecuted, and punished under domestic laws. These threats helped minimize an otherwise unregulated activity. In cyberspace, however, spies can access far more information and data with far less personal risk, upsetting the imperfect but at least established standing equilibrium.

Even when a state identifies and reasonably attributes cyberespionage to another state, it has few effective and non-escalatory options. Should it issue criminal indictments of suspected individuals, as the United States did with members of China's People's Liberation Army?[179] Or should it attempt to embarrass the allegedly responsible state, by naming and shaming? Or should it take some covert response? All of these approaches have significant drawbacks: criminal indictments will usually be unenforceable; naming and shaming carries little weight with regard to espionage, given that all states are engaged in similar activities; responsive offensive covert countermeasures are likely themselves unlawful due to the notice requirement[180] and their invisibility contributes to the perception that cyberspace is a lawless zone while simultaneously risking conflict escalation.

But what if states could be held liable for the harm associated with discovered or publicized cyberespionage? There would be no need to determine the lawfulness of the cyberoperation; rather, the injuries associated with the activity would raise the possibility of state liability. The harms associated with these discovered or publicized cyberoperations are usually significant, suggesting that these acts could be identified as international cybertorts, triggering state liability and a duty to compensate. While hardly a magic bullet for the asymmetry of cyberespionage, recognizing such activities as international cybertorts presents victim states with a new means of responding.

---

tent/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/9AL3-8JHU].

179 Mark Landler & David E. Sanger, *Hacking Charges Threaten Further Damage to Chinese-American Relations*, N.Y. TIMES, May 22, 2014, at A14.

180 *See* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1, 2 n.11 (2017) (discussing legal restrictions on covert countermeasures, including the requirement of prior or subsequent notice); *see also* TALLINN MANUAL 2.0, *supra* note 46, r. 21 cmt. 10 (elaborating on the notice requirement); *id.* r. 21 cmt. 12 (noting situations where notice may not be required).

Clearly, there are a number of benefits that would attend expanding the principle of state liability to cyberoperations that cause significant transboundary harm. Before it can be employed, however, certain questions will need to be resolved.

3. *State Liability in Cyberspace: Questions to Be Considered*

This section provides an initial sketch of the main conceptual questions that will need to be addressed to develop a principle of state liability for transboundary harm in cyberspace: What constitutes "significant harm"? What duties does a state owe (or should owe) other states in cyberspace? How should causation be evaluated? What standard of liability should be applied?[181]

a. *What Constitutes Significant Harm?*

Because this Article's definition of international cybertort relies on "significant harm" as a limiting factor, much will depend on what level and kinds of harm are "significant."[182] Thousands of damaging cyberoperations occur on a daily basis[183]—what level of injury is necessary? A thousand dollars' worth of damage? A million? Ten million? Is this an objective assessment, or will the understanding of what is significant depend on the wealth of the attacked entity? Should more abstract harms—such as interference in an election—be recognized and addressed?[184] Domestic tort law certainly recognizes a wide variety of harms, including violations of property or constitutional rights as well as physical, emotional, and

---

181 More instrumental questions—such as how this legal regime should be developed and enforced—are considered in Part IV.

182 Many conventions refer to "significant," "serious," or "substantial" harm or damage to delineate the threshold for legal claims. *See, e.g.*, Draft Principles on the Allocation of Loss 123 (2006) ("The term 'significant' is understood to refer to something more than 'detectable' but need not be at the level of 'serious' or 'substantial.'" (emphasis omitted)).

183 *See, e.g.*, NORSE INTELLIGENCE PLATFORM, http://map.norsecorp.com [https://perma.cc/WT4B-Z3PU] (showing cyberattacks in real time); FIREEYE CYBER THREAT MAP, https://www.fireeye.com/cyber-map/threat-map.html [https://perma.cc/726X-P49D] (counting the number of cyberattacks each day); CYBERTHREAT REAL TIME MAP, https://cybermap.kaspersky.com [https://perma.cc/4FJD-CUM3] (sorting cyberthreats in real time by most-attacked countries); DIGITAL ATTACK MAP, http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16702&view=map [https://perma.cc/4FC3-M2Q8] (showing top daily worldwide Distributed Denial of Service attacks).

184 For an exploration of the different kinds of harms associated with data breaches, see Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638 [https://perma.cc/A9C2-EMTF].

reputational injuries. There might be a similar panoply of more abstract harms at the international level. The U.S. Department of Defense's (DoD) Cyber Strategy showcases the potential breadth of the concept. It states that the DoD has an obligation to "defend the United States and its interests against cyberattacks of significant consequence," regardless of whether they constitute cyberwarfare.[185] While noting that cyberincidents will be "assessed on a case-by-case and fact-specific basis," it declares that "significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[186]

As with many other questions of evaluating and valuing tort violations, these are questions best left to the "jury"—which, in the international legal order, is comprised of the community of states.[187] States, like plaintiffs in domestic law, will determine what injuries they will absorb and which are worth challenging; other states' responses to such accusations will be instrumental in developing norms about what constitutes significant harm.[188] Indeed, as is often the case in international technological regulation, the inherent ambiguity of "significant harm" is a strength: it is a relatively tech-neutral standard that permits coherent but flexible legal development.[189]

b. *What Duties Do States Owe Other States?*

Much depends on the question of what duties a state owes (or should owe) other states. Any claim that a state is liable for transboundary harm associated with a cyberoperation must first demonstrate that states have (1) a duty not to cause transboundary harm in cyberspace; (2) a duty to prevent or mitigate the causation of transboundary harm in cyberspace, which might also be characterized as a duty of due diligence; and/or (3) a duty to compensate for transboundary harm caused by their cyberoperations or that occurs due to a lack of due dili-

185 U.S. DEP'T OF DEFENSE, THE DEPARTMENT OF DEFENSE CYBER STRATEGY 5 (2015).

186 *Id.*

187 Alternatively, should states establish an independent tribunal, a group of experts could be appointed to evaluate claims. *See infra* subpart IV.C.

188 *See* Crootof, *Change Without Consent*, *supra* note 120, at 256 (explaining when state party conduct becomes subsequent practice).

189 *Cf.* Rebecca Crootof, *A Meaningful Floor for "Meaningful Human Control,"* 30 TEMPLE INT'L & COMP. L.J. 53, 58–60 (2016) (arguing that, because it allows for flexible and responsive interpretation, the imprecision of the "meaningful human control" principle is beneficial, provided that it is bounded by an interpretative floor).

gence. These three conceptions of state duties might be understood as interrelated or completely independent.

A duty not to cause transboundary harm is fairly self-explanatory: states would have a duty not to engage in any activities that result in transboundary harm. A duty not to cause transboundary harm is distinct from a duty to prevent the causation of transboundary harm; the former would apply only to state and state-sponsored activities, while the latter is a more general obligation on states to monitor and limit what other states and non-state actors do on their territory or within their jurisdiction or control. Under the former conception, North Korea would have had a duty not to engage in potentially harmful cyberoperations against the United States; under the latter, it would have had a duty to prevent other states or non-state actors from engaging in such activities anywhere within its jurisdiction or control.

The second option—a duty to prevent the causation of transboundary harm—might also be characterized as a duty of due diligence. There is some precedent for this concept in international jurisprudence. In the *Pulp Mills* case, the ICJ found that all states have

> [a]n obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party. It is an obligation which entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement and the exercise of administrative control applicable to public and private operators . . . to safeguard the rights of the other party.[190]

More and more, scholars are discussing due diligence as an independent standard for evaluating appropriate state action in cyberspace. Michael Schmitt argues that states should shoulder additional due diligence obligations in cyberspace, given that they have a "due diligence obligation with respect to both government and private cyber infrastructure on, and cyber activities emanating from, their territory."[191] The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* has two rules regarding due diligence, recognizing it as a general principle and applying it in the cyber context.[192]

---

190 Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. Rep. 14 (Apr. 20) at 69, ¶ 197.

191 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. FORUM 68, 70 (2015), http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace [https://perma.cc/BE9D-3YUY].

192 Rule 6 provides, "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be

A due diligence standard might span a spectrum of requirements. What might be characterized as a "strong" due diligence standard—a general duty to prevent others from causing transboundary harm—carries the risk of creating an incentive for states to exercise complete control over information technologies. This is exactly what the Shanghai Cooperation Organization states have been advocating, and exactly what Western states have been resisting in the interest of preserving freedom of expression and the free exchange of information on the internet.[193] As Jack Goldsmith has noted, while questioning the likelihood of a cybersecurity treaty,

> The United States might one day be willing to accept comprehensive U.S. government monitoring and 24/7 real-time police or military pursuit in the private network in exchange for a serious clamp-down on malicious activity from Russia and China. But the idea is unthinkable today. . . . What we need to do to protect ourselves in the cyber realm is in deep conflict with our commitments to limited government and private control of the communications infrastructure.[194]

In contrast, a relatively "weak" due diligence duty would arise only with regard to known harms: states should be expected to take only reasonably feasible measures to minimize those harms, and there should be no duty to monitor networks and no duty of prevention.[195]

There is recent state practice that could be understood as supporting a duty of due diligence. In early 2017, a variant of the WannaCry ransomware "crippled 200,000 computers in more than 150 countries,"[196] making it the largest known ransomware assault to date.[197] The malware employed a hacking tool called "Eternal Blue," which was originally developed by

---

used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." TALLINN MANUAL 2.0, *supra* note 46, r. 6. Rule 7 states, "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States." *Id.* at r. 7.

193 JACK GOLDSMITH, CYBERSECURITY TREATIES: A SKEPTICAL VIEW 4 (2011).

194 *Id.* at 9.

195 *Cf.* TALLINN MANUAL 2.0, *supra* note 46, r. 6–7 (requiring states to take actions "feasible in the circumstances" to comply with the due diligence principle). *See generally* Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016) (arguing that private sector cybersecurity due diligence practices can inform the international due diligence discussion).

196 Goldman, *supra* note 132.

197 *See* Perlroth & Sanger, *supra* note 131 ("The attacks appeared to be the largest ransomware assault on record.").

the NSA and subsequently leaked by a hacking group called the "Shadow Brokers."[198] While there is growing evidence that the attacks are linked to North Korean hackers,[199] China has blamed the United States for the attack, presumably on the rationale that the United States had allowed a dangerous tool to fall into the wrong hands or had not taken sufficient action to minimize the harm associated with its leaked tool.[200] The NotPetya malware attacks also used Eternal Blue, resulting in similar calls for NSA to "help the rest of the world defend against the weapons it created."[201]

Finally, states may have a duty to compensate victims for any harms caused by their cyberoperations and/or caused by inadequate due diligence.[202] This could be understood as a natural corollary of a duty to not cause transboundary harm or a duty of due diligence, where a lapse would trigger a duty to compensate. Alternatively, there may be a general presumption that states may engage in activities not prohibited by international law even if doing so causes transboundary harm, provided that the state subsequently compensates victims for any associated harms. The *Lotus* case—which held that state actions not expressly prohibited under international law are permitted[203]—would support this more limited conception, and given state interest in preserving room to play, this is the most likely candidate for general adoption.

c. *How Should Causation Be Evaluated?*

A second limiting factor will be whether a given state can be determined to have caused an international cybertort. Causa-

---

198 *Id.*

199 Nicole Perlroth, *More Evidence Points to North Korea Role in Global Ransomware Attack*, N.Y. TIMES, May 23, 2017, at B4 (including the fact that the "WannaCry attacks used the same command-and-control server used in the North Korean hack of Sony Pictures Entertainment in 2014").

200 Paul Mozur & Jane Perlez, *Evidence Links North Korea to Cyberattack, but China Stays Mute*, N.Y. TIMES, May 18, 2017, at A8 ("Despite evidence suggesting a North Korean role in the ransomware attack, the most common reaction among experts and on Chinese social media was to blame the United States.").

201 Perlroth, Scott & Frenkel, *supra* note 126.

202 In other words, a duty not to cause transboundary harm might be understood as a liability rule. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

203 S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7) (observing that, because of the consensual nature of the international legal order, "Restrictions upon the independence of States cannot be therefore be presumed."). *But see* Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. Rep. 404, ¶ 8 (July 22) (declaration of Judge Simma) (criticizing the famous *Lotus* dictum as an outdated, "excessively deferential" approach).

tion is hardly a simple legal concept, but it is at least a familiar one with well-traced complications. And, as in domestic tort law, establishing whether a given act caused a given harm will necessarily be a fact-specific analysis.

Causation of significant harm (the state liability standard) is fundamentally different from attribution of an internationally wrongful act (the state responsibility standard):

> [I]nternational liability of a State associated with its obligation not to cause harm to other States requires no attributability of the act to the State. . . . International liability arises out of injurious consequences which, according to the natural law of causation, must result from activities over which the State has or should have direct or indirect control or that lie within its jurisdiction.[204]

Given this, it seems likely that "causation" will be interpreted far more broadly than "attribution" with regard to the activities of non-state actors[205]—especially if states are understood as having a due diligence obligation.

Eric Talbot Jensen and Sean Watts have suggested that a duty of due diligence may help mitigate the attribution problem.[206] Imagine a scenario where State A is the victim of a malicious cyberoperation conducted by State B, which is routed through State C's cyber infrastructure. While State A can determine the cyberoperation came from State C, it cannot reasonably identify the original perpetrator. Absent a due diligence duty, State A could not hold States B or C responsible nor engage in countermeasures against either; with a due diligence duty, State A could inform State C of the harm and, should State C fail to take reasonable actions to end it, State C would have committed an internationally wrongful act permitting State A to engage in countermeasures against State C.[207] However, as Jensen and Watts recognize, this potential benefit comes with attendant costs.[208] This conception of due diligence expands both when and against whom a victim state

---

204 Sucharitkul, *supra* note 148, at 834–35.

205 The state responsibility attribution standard for the activities of non-state actors is extremely circumscribed. *See infra* section II.B.2.

206 Jensen & Watts, *supra* note 82.

207 *Id.* at 1567–68.

208 *Id.* at 1568 (observing that a due diligence standard might contribute to the "erosion of State internalization of international law, proliferation of resorts to self-help, hindrance of multilateral and collective capacity, and faulty assignments of culpability").

might use countermeasures, risking increased conflict escalation.[209]

But if due diligence is understood as expanding the number of states that could be held liable for compensation, as opposed to responsible for an internationally wrongful act justifying the use of countermeasures, some of the problems Jensen and Watts identify with expanding attribution would be minimized. Assigning liability, rather than responsibility, for due diligence violations might reduce state resort to self-help measures[210] and make multilateral solutions more attractive.[211]

d. *What Standard of Liability Should Apply?*

Finally, what standards of liability should be applied in evaluating state liability for international cybertorts? As in domestic tort law, there are good reasons to employ different standards for different levels of intent, as there are fundamental differences between unforeseeable accidental damage, likely accidental damage, non-accidental damage, and intentional damage.[212]

Certainly, a state should be held liable for intended harms and for harms resulting from its ultrahazardous activities. Intentional torts and ultrahazardous activities—those that involve a risk of "significant transboundary harm, which is either unforeseeable or, if foreseeable, is unpreventable even if a state takes due care"—are almost always evaluated under a strict liability standard.[213]

States should also be held at least partially liable for unintended harms resulting from their not-unlawful activities, though the appropriate standard of liability is less obvious.

---

209 *Id.* at 1577 ("In short, by presenting more opportunities for more States to allege more breaches of international law, due diligence potentially increases the frequency of States' resort to countermeasures and their accompanying potentially destabilizing effects.").

210 *Id.* at 1573–74.

211 *Id.* at 1574–75. Admittedly, however, this substitution of state liability for state responsibility does little to address the fact that this is "a *proxy* approach," whereby the perpetrator can completely evade consequences, *id.* at 1575, and it may even exacerbate the problem of rule erosion, to the extent it encourages states to engage in "efficient breaches," *id.* at 1568–73.

212 Whether a state should be held vicariously liable for the actions of non-state actors or other states operating on its territory or employing devices within its jurisdiction or control will depend first on whether a duty to prevent the causation of transboundary harm is established. *Supra* subsection II.C.3.b.

213 Malgosia Fitzmaurice, *International Responsibility and Liability*, *in* OXFORD HANDBOOK OF INTERNATIONAL ENVIRONMENTAL LAW 1010, 1022 (Daniel Bodansky, Jutta Brunnée, Ellen Hey eds., 2008).

Some suggest that "liability of a State may be said to be strict or almost absolute, regardless of fault, intention or negligence, for activities within its jurisdiction or on a sea-going vessel or spacecraft carrying its flag or registered in its territory."[214] A strict liability standard certainly simplifies the liability analysis: if it can be determined that a state's action or inaction caused transboundary harm, the state will be liable for the costs associated with that harm. There are also arguments for a lesser standard of liability for harms resulting from negligence or from socially-useful activities. Walton contends that "due diligence" is best understood as a standard of liability, rather than as a freestanding independent duty,[215] and that it provides the appropriate standard when evaluating unintentional harms associated with socially-useful activities.

Oren Gross has also proposed that the state victim to a harmful cyberoperation should bear some liability for failures to take appropriate cybersecurity measures.[216] A victim state's particularly egregious cybersecurity practices might be treated as a kind of contributory or comparative negligence that mitigates another state's liability for its international cybertorts.

* * * * *

A cyberoperation like the Sony hack does not fit squarely into the transnational cybercrime nor the cyberwarfare categories. Instead, it is conceptually and legally useful to identify the Sony hack as an international cybertort. Shifting to a tort-law framework also highlights the benefits of applying the principle of state liability for transboundary harms to state action in cyberspace.

However, there is another aspect to cyberoperations like the DNC hack worth discussing: in addition to being cyber-espionage that cost the DNC hefty sums, the action was likely also intended to sow confusion and possibly even alter the outcome of a U.S. presidential election. While the DNC hack may not have been itself unlawful, imagine if Russian actors instead hacked voting machines and altered individual votes. If such an action caused significant harm, it might be an inter-

214 *See* Sucharitkul, *supra* note 148, at 835.

215 Walton, *supra* note 17, at 1497 ("If due diligence is the appropriate standard by which to judge state conduct at the level of low-intensity cyber attacks, then such an approach would have to recognize the underlying duty to prevent transboundary harm—given that this is the only primary duty that governs the low-intensity space.").

216 Gross, *supra* note 59.

national cybertort. But it would also be something more—unlawful interference.[217]

III
STATE RESPONSIBILITY FOR INTERNATIONALLY WRONGFUL ACTS

In contrast to the principle of state liability for transboundary harm, the law of state responsibility holds states accountable for their internationally wrongful acts. After a brief review of the law of state responsibility, this Part considers two kinds of unlawful interference—violations of state sovereignty and intervention—that would ordinarily trigger the applicability of state responsibility, and then discusses how cyberspace facilitates such activities. It concludes that, instead of expanding existing definitions of internationally wrongful acts to cover these cyber-enabled interferences, states should use the possibility of state liability to deter such cyberoperations.

A. The Law of State Responsibility

The law of state responsibility is intended to create accountability mechanisms for states that engage in any "internationally wrongful act," defined as "conduct consisting of an action or omission" that "constitutes a breach of an international obligation of the State" and "is attributable to the State under international law."[218] If a state is responsible for an internationally wrongful act, it is obligated to make full reparation.[219]

1. *Breach of an International Obligation*

From its inception, the ILC's focus in codifying the law of state responsibility was limited to the topic of wrongful acts. According to the Draft Articles, "The essence of an internationally wrongful act lies in the non-conformity of the State's actual conduct with the conduct it ought to have adopted in order to comply with a particular international obligation."[220] The conduct a state "ought to have adopted" might be found in customary international law, treaty law, or general principles of the

---

217 Egan, *supra* note 178 ("[A] cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention.").

218 Draft Articles, *supra* note 47, art. 2.

219 *Id.* art. 31.

220 *Id.* ch. 3 cmt. 3.

international legal order.[221] However, an act is not a breach of an international obligation "unless the State is bound by the obligation in question at the time the act occurs."[222] The number and kind of internationally wrongful acts a state can engage in is limited only by its international obligations.[223]

Additionally, if the law evolves such that states are understood to have a duty to compensate those harmed by their international cybertorts, the failure to provide compensation might itself constitute an internationally wrongful act triggering the applicability of the law of state responsibility and its broader remedial measures.[224]

2. *Attribution*

"Attribution," in the state responsibility context, "denote[s] the operation of attaching a given action or omission to a State."[225] Certainly, the actions of state organs are attributable to a state.[226] States may be held responsible both for the actions of those non-state actors that are *de facto* state organs,[227] as well as for the actions of non-state actors acting "on the instructions of, or under the direction or control of" a state in carrying out an operation.[228]

The standard for determining when attribution for *de facto* state organs is appropriate remains unresolved. The ICJ has adopted a "strict control" test, while the International Criminal Tribunal for the Former Yugoslavia (ICTY) has employed a rela-

---

221 *Id.*

222 *Id.* art. 13.

223 Notwithstanding those who maintain that there are no rules in love or war, violations of the law of armed conflict are taken seriously. The *Tallinn Manual 2.0* meticulously details how these rules apply to state action in cyberspace—arguably to the detriment of other relevant areas of law. *See* Rebecca Ingber, *Interpretation Catalysts in Cyberspace*, 95 TEX. L. REV. 1531 (2017).

224 *Supra* section II.C.1.

225 Draft Articles, *supra* note 47, art. 2 cmt. 12.

226 *See id.* art. 4 ("1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State. 2. An organ includes any person or entity which has that status in accordance with the internal law of the State."). The ICJ has recognized this Article as customary international law. *See* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 385 (Feb. 26).

227 Draft Articles, *supra* note 47, art. 4.

228 *Id.* art. 8. The "three terms 'instructions', 'direction' and 'control' are disjunctive; it is sufficient to establish any one of them." *Id.* art. 8 cmt. 7.

tively relaxed "overall control" standard.[229] If a non-state actor is a *de jure* or *de facto* state organ, the state will be responsible for all of its actions, regardless of whether they are *ultra vires*.[230]

Additionally, the acts of non-state actors may also be attributable to a state under Article 8 of the Draft Articles, which holds that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[231] In the Draft Articles, the ILC adopted the ICJ's "effective control" test for Article 8 attribution.[232] Under this standard, a state will only be held responsible for actions that occur in the context of an operation over which it exercises effective control,[233] and it will only be responsible for a non-state actor's *ultra vires* actions that are "an integral part" of the operation.[234]

The *Tallinn Manual 2.0* ties state responsibility for a non-state actor's cyberoperation to the ICJ's "effective control" test under Article 8.[235] As many scholars have argued, however, this standard (and other tests for attribution) may be inappro-

---

229 For the ICJ's "strict control" test, see *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. at ¶ 391; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 109–10 (June 27) (using the phrase "complete dependence" to refer to a similar control standard). For the ICTY's "overall control" test, see Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber, Judgment, ¶ 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

The Draft Articles discuss the "overall control" test as a standard of attribution under Article 8. *See* Draft Articles, *supra* note 47, art. 8 cmt. 5. For a discussion of why it is better conceived of as a standard of attribution under Article 4, see EMILY CHERTOFF, LARA DOMÍNGUEZ, ZAK MANFREDI & PETER TZENG, STATE RESPONSIBILITY FOR NON-STATE ACTORS THAT DETAIN IN THE COURSE OF A NIAC 21 (2015) [hereinafter State Responsibility White Paper], https://law.yale.edu/system/files/yls_glc_state_responsibility_for_nsas_that_detain_2015.pdf [https://perma.cc/55JK-LWK8]; *id.* 21 nn. 130–31 (citing supporting sources).

230 Draft Articles, *supra* note 47, art. 7; *id.* art. 7 cmts. 1–8 (describing supporting state practice and judicial decisions); *see also Prosecutor v. Tadić*, Judgment, ¶¶ 121, 123 (holding that "a State is internationally accountable for *ultra vires* acts or transactions of its organs [and that the State] incurs responsibility even for acts committed by its officials outside their remit or contrary to its behest").

231 Draft Articles, *supra* note 47, art. 8. The ICJ has recognized this as reflecting customary international law. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. ¶ 398.

232 Draft Articles, *supra* note 47, art. 8, cmts. 3–5.

233 State Responsibility White Paper, *supra* note 229, at 27–28.

234 Draft Articles, *supra* note 47, art. 8 cmt. 3.

235 *See* TALLINN MANUAL 2.0, *supra* note 46, r. 17 cmt. 6 ("A State is in 'effective control' of a particular cyber operation by a non-State actor whenever it is the State that determines the execution and course of the specific operation and the

priately high for determining state-sponsored cyberoperations carried out by non-state actors.[236] Attributing the acts of non-state actors to states is never an easy undertaking, and it is complicated in cyberspace by the opportunities for anonymity and misdirection.

Ultimately, absolute certainty regarding attribution is rarely possible; instead, a state seeking to hold another responsible for an internationally wrongful act is expected to independently judge a variety of facts to make a reasonable determination as to whether there is justification for attribution.

3. *Reparations*

Once an internationally wrongful act is attributable to a state, the state is then "under an obligation to make full reparation for the injury caused by the internationally wrongful act."[237] The concept of reparation under the law of state responsibility is far broader than the compensation suggested by the principle of state liability. Reparation might "take the form of restitution, compensation and satisfaction, either singly or in combination."[238] Restitution requires "re-establish[ing] the situation which existed before the wrongful act was commit-

---

cyber activity engaged in by the non-State actor is an 'integral part of that operation.'").

236 *See, e.g.*, Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 549–50 (2012) (arguing that a victim state may use force against a state that refuses to prevent malicious cyberoperations emanating from its territory); Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 890 (2012) (arguing that a victim state should be able to use force against states that are "directly or indirectly" involved in a non-state actor's cyberoperations); Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELBOURNE J. INT'L L. 496, 496 (2013) (proposing a "virtual control" standard, which would "impos[e] responsibility on a state that has provided financial or other assistance to private groups" and shift the burden of proof to the accused state); 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 MILITARY L. REV. 1 (2009) (arguing that states may use force against third-party states who do not take sufficient precautions against their servers being used for cyberoperations). *But see* Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, 1 FLETCHER SECURITY REV. 53, 65 (2014) (suggesting that the existing standards will remain high).

237 Draft Articles, *supra* note 47, art. 31. The 2005 Basic Principles expand this list to include rehabilitation and guarantees of non-repetition. Basic Principles, *supra* note 46, ¶ 18; *see also* Draft Articles, *supra* note 47, art. 30(b) (imposing an obligation on a state responsible for an internationally wrongful act to offer guarantees of non-repetition).

238 Draft Articles, *supra* note 47, art. 34.

ted."[239] Monetary compensation is required to the extent damage is not made good by restitution.[240] Satisfaction—which may entail acknowledging the breach, expressing regret, or a formal apology—is required to the extent the damage cannot be made good by restitution or compensation.[241] The appropriate form of restitution will depend on the kind and scope of the harm, and of course, full reparation may not always be possible.

B. Cyber-Facilitated Interference

States regularly attempt to influence other states' actions in myriad ways—through economic aid and sanctions, propaganda, political maneuvering, and shows of military force. International law permits many such influences, but recognizes two kinds of interference—violations of state sovereignty and intervention—as internationally wrongful acts.[242] When attributable to a state, such unlawful interferences trigger the law of state responsibility.

While these concepts are well-established in principle, their scope is often unclear. Furthermore, given how cyberspace facilitates interference and that states are reluctant to term such activities internationally wrongful acts, the line between lawful and unlawful interference is becoming further blurred.

1. *Unlawful Interference: Violations of State Sovereignty and Interventions*

State sovereignty is one of the foundational concepts of the international legal order. As articulated by Max Huber in the 1928 Island of Palmas arbitral award, "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[243]

---

239 *Id.* art. 35.

240 *Id.* art. 36.

241 *Id.* art. 37. Interest may be necessary to ensure full reparation. *See id.* art. 38.

242 While the terms "interference" and "intervention" are sometimes used interchangeably, it is useful to distinguish between them. Interference encompasses both lawful and unlawful meddling; intervention is coercive and therefore prohibited. *See* 1 OPPENHEIM'S INTERNATIONAL LAW 432, 433–34 (Sir Robert Jennings & Sir Arthur Watts eds., 9th ed. 2008) [hereinafter OPPENHEIM].

243 Island of Palmas (Neth. v. U.S.) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928). The *Tallinn Manual 2.0* conceives of state sovereignty as having an internal and external component and, by extension, divides potential violations of state sovereignty into two categories: "(1) the degree of infringement upon the target State's

The U.N. Charter consecrates the concept, grounding its legitimacy "on the principle of the sovereign equality of all its Members."[244]

The customary prohibition on intervention forbids "all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[245] This prohibition is well-established in international law, with some even going so far as to consider it *jus cogens*.[246] It was first codified in a multilateral treaty in the 1933 Montevideo Convention: "No state has the right to intervene in the internal or external affairs of another."[247] Although the prohibition on intervention is not specifically mentioned in the U.N. Charter,[248] post-Charter institutions have regularly reaffirmed it;[249] the ILC noted it in its draft articles on the rights and duties of states;[250] the U.N.

---

territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions." TALLINN MANUAL 2.0, *supra* note 46, r. 4 cmt. 10; *see id.* r. 2; *id.* r. 3).

244 U.N. Charter art. 2, ¶ 1.

245 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27); *see also id.* ¶ 209 (holding that, where interference takes the form of a use or threat of force, Article 2(4) and the customary norm of non-intervention are coterminous).

246 Watts, *supra* note 20, at n.27 (citing sources).

247 Montevideo Convention on the Rights and Duties of States art. 8, Dec. 26, 1933, 49 Stat. 3097, T.S. No. 881.

248 While the principle of state sovereignty can be read to include the principle of non-intervention, as a formal matter the U.N. Charter only explicitly prohibits intervention by itself or other U.N. bodies. U.N. Charter art. 2, ¶ 7 ("Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.").

249 *See, e.g.*, Charter of the Organization of American States art. 18, Feb. 27, 1967, 33 I.L.M. 987 ("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.").

250 Draft Declaration on Rights and Duties of States with Commentaries, Int'l L. Comm'n Rep. on the Work of Its First Session, art. 3, G.A. Res. 375 (IV) (Dec. 6, 1949) ("Every State has the duty to refrain from intervention in the internal or external affairs of any other State.").

General Assembly has issued a number of resolutions reiterating it;[251] and the ICJ regularly acknowledges it.[252]

The prohibition on intervention can be understood as flowing directly from the concept of state sovereignty: if states have a right to the independent, exclusive exercise of state functions, other states are necessarily prohibited from taking coercive actions that would impair that right.[253] According to one reading, the prohibition on intervention protects the non-territorial, "metaphysical aspect of sovereignty (a state's political integrity) rather than its physical dimension (a state's territory)."[254]

Alternatively, violations of sovereignty and intervention can be understood as separate categories of internationally wrongful acts that, while clearly related, do not completely overlap.[255] Certainly, there are acts that could be considered sovereignty

---

251 *See, e.g.*, G.A. Res. 50/172, Resolution on Respect for the Principles of National Sovereignty and Non-interference in the Internal Affairs of States in Their Electoral Processes, U.N. Doc. A/RES/50/172 (Feb. 27, 1996) ("[T]he principles of national sovereignty and non-interference in the internal affairs of any State should be respected . . . ."); G.A. Res. 37/10, Resolution on the Peaceful Settlement of Disputes Between States, U.N. Doc. A/RES/37/10 (Nov. 15, 1982) ("Reiterating that no State or group of States has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State . . . ."); G.A. Res. 36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, U.N. Doc. A/Res/36/103 (Dec. 9, 1981) (listing the rights and duties associated with the principle of non-intervention and non-interference); G.A. Res. 25/2625, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970) ("[T]he obligation not to intervene in the affairs of any other State is an essential condition to ensure that nations live together in peace . . . .").

252 *See, e.g.*, Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 163 (Dec. 19) ("The Court considers that the obligations arising under the principles of non-use of force and non-intervention were violated by Uganda . . . ."); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 242 (June 27) ("The Court therefore finds that the support given by the United States . . . constitutes a clear breach of the principle of non-intervention."); Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, ¶ 121 (Apr. 9) ("The Court can only regard the alleged right of intervention as the manifestation of a policy of force, [which] . . . cannot, whatever be the present defects in international organization, find a place in international law.").

253 *Cf. Nicar v. U.S.*, 1986 I.C.J. at ¶ 205 (stating that the prohibition on intervention forbids states from meddling in "matters in which each State is permitted, by the principle of State sovereignty, to decide freely").

254 Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 65, 78 (Anna-Maria Osula & Henry Rõigas eds., 2016).

255 *See* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1653–54 (2017).

violations that do not seem to meet the standard for interventions: there is a strong argument that the Sony hack constituted a violation of U.S. sovereignty, although it was not sufficiently coercive to qualify as an intervention.[256] It is harder, however, to conceive of an intervention that would not also violate a state's sovereignty, given that coercive interference in a state's affairs would necessarily constitute a significant "interference with or usurpation of inherently governmental functions."[257]

2. *An Elusive Line Between Lawful and Unlawful Interference*

Both state sovereignty and the prohibition on intervention are well-established in principle, but the scope of their application resists clear codification. This is largely due to the fact that adjudications of these issues tend to be fact-specific. Furthermore, states and experts are divided on whether it is appropriate to apply older concepts to new kinds of technologically-facilitated interference.

a. *State Sovereignty*

The difficulty in defining the scope of what constitutes a violation of state sovereignty is illustrated by the *Tallinn Manual 2.0* experts' inability to agree on its borders. Most of the experts agreed that "cyber operations constitute a violation of sovereignty in the event they result in physical damage or injury, as in the case of malware that causes the malfunctioning of the cooling elements of equipment, thereby leading to overheating that results in components melting down" and that "the causation of physical consequences by remote means on that territory likewise constitutes a violation of sovereignty."[258] However, the experts could not reach consensus on the question of whether "a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty."[259]

Similarly, there are competing arguments regarding whether the DNC hack would constitute a violation of U.S. sovereignty. Assuming that it can be attributed to Russia, some would characterize it as a sovereignty violation because it

---

256 Schmitt, *supra* note 8 (arguing that simply "[d]isrupting a private company's activities" is not sufficiently coercive to qualify as an intervention).

257 TALLINN MANUAL 2.0, *supra* note 46, r. 4 cmt. 10.

258 *Id.* r. 4 cmt. 11.

259 *Id.* r. 4 cmt. 14.

involved nonconsensual intrusion into U.S. cyberinfrastructure.[260] However, there is a minority viewpoint that "mere compromises or thefts of data are not violations of sovereignty, but rather routine facets of espionage and competition among States."[261]

Further complicating matters, senior U.S. officials have recently argued there is no overarching rule against violations of sovereignty in international law. Instead, they claim that there is a general principle that state sovereignty is to be respected, but this principle takes different forms in different forums, and the rules for cyber are still in flux.[262]

b. *Intervention*

The prohibition on intervention has also resisted clear delineation.[263] First, it is not obvious what state activities are shielded from outside interference. The ICJ has stated that protected state affairs include "choice of a political, economic, social and cultural system, and the formulation of foreign policy";[264] according to a more recent Chatham House report, prohibited activities might also include, depending on the circumstances, "[i]nterference in political activities," "[s]upport for secession," and "[s]eeking to overthrow the government—so-called 'regime change.'"[265] The concept of the *domaine réservé* helps describe what state activities are protected from intervention, but the "displacement of a matter or issue from the *domaine réservé* does not constitute an overall eradication or waiver of the principle of non-interference, nor an open sea-

260 *See* Watts, *supra* note 10.

261 *Id.* Regarding this, Ryan Goodman has made an interesting and somewhat counterintuitive point: if the misappropriation and distribution of information associated with the DNC hack is not a violation of international law—if it is not a violation of state sovereignty or intervention—the practice could be employed unilaterally as a punitive retorsion. Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SECURITY (Jan. 5, 2017, 8:01 AM), https://www.justsecurity.org/35999/international-law-response-russian-election-interference [https://perma.cc/S3KM-B8JC]. Retorsions are politically unfriendly but lawful self-help measures. *Supra* note 55.

262 For an argument in favor of this understanding, see Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017). Gary Corn is the Staff Judge Advocate of the U.S. Cyber Command, and Robert Taylor is the former Principal Deputy General Counsel of the U.S. Department of Defense. For a responsive critique, see Schmitt & Vihul, *supra* note 255, at 1668–70.

263 CHATHAM HOUSE, THE PRINCIPLE OF NON-INTERVENTION IN CONTEMPORARY INTERNATIONAL LAW 3, 6 (2007).

264 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 205 (June 27).

265 CHATHAM HOUSE, *supra* note 263, at 7.

son on influencing conditions in another state's territory."[266] Ultimately, there is no definitive list of what state affairs are and are not protected.[267]

Second, lawful interference is often distinguished from prohibited intervention based on the degree of coercion exercised.[268] But what constitutes coercion? Oppenheim defines unlawful intervention as that which is "forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."[269] Dispatching armed forces to another state will certainly constitute prohibited intervention; it is less clear whether and when economic, political, and psychological pressures are sufficiently coercive to satisfy the legal requirement for prohibited intervention.[270]

Confusion in the doctrine is leading some states to exploit the grey areas and others to err on the side of repression. Consider Ecuador's reaction to the DNC hack. WikiLeaks founder Julian Assange has been living in exile in Ecuador's London embassy since 2012, avoiding a Swedish rape investigation which he believes to be the cover story for an American extradition.[271] With the expressed intent of hobbling WikiLeaks' interference in the 2016 U.S. general election and to evade any hint of responsibility for facilitating unlawful interventions, Ecuador cut Assange's internet access.[272] However, the controversial leaked emails were originally obtained by Russian hackers, not Assange or Ecuador[273]—and while their disclosure likely constituted disfavored interference, it probably was not sufficiently coercive to meet the definition for unlawful intervention.

---

266 Watts, *supra* note 20, at 265.

267 *Id.*

268 The ICJ identified "coercion" as the element "which defines, and indeed forms the very essence of, prohibited intervention." *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 205.

269 OPPENHEIM, *supra* note 242, at 432; *see also* TALLINN MANUAL 2.0, *supra* note 46, r. 66 cmt. 21 ("The key is that the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take).").

270 There is a minority view that Article 2(4) prohibits political and economic coercion; the majority understanding is that it prohibits only threats or uses of force. Hathaway et al., *supra* note 77, at 842.

271 Steven Erlanger & David E. Sanger, *Ecuador Cuts Link to the Internet*, N.Y. TIMES, Oct. 19, 2016, at A1.

272 The government of Ecuador stated that it "respects the principle of nonintervention in the affairs of other countries" and that "it does not interfere in the electoral processes in support of any candidate in particular." *Id.*

273 *Id.*

Given these ambiguities, a determination of whether a given act constitutes a prohibited violation of state sovereignty or unlawful intervention necessitates a fact-specific inquiry, focused on the existence, validity, and scope of state consent; the degree and kind of coercive activity; and whether any coercive acts by a non-state actor can be attributed to another state.[274] Unfortunately, cyberspace facilitates interference while simultaneously confusing the facts relevant to categorization.

3. *Increased Likelihood of Interference*

The U.S. attribution of the DNC hack to Russia reignited an ongoing conversation regarding whether and how foreign actors may use new technologies in an attempt to influence elections.[275] Such cyber-enabled acts might range from publicizing hacked private communications to disseminating misinformation to exploiting voting machine vulnerabilities to manipulating social media.[276] Nor are these pure hypotheticals: states have long used cyberoperations to influence elections,[277] and U.S. security experts and non-governmental organizations have recently identified areas of the electoral infrastructure that are particularly vulnerable to tampering.[278]

---

274 The issue is further confused by recent calls to establish a doctrine of humanitarian intervention, under which states would be permitted to unilaterally use force to stop an ongoing mass atrocity. Crootof, *Change Without Consent*, *supra* note 120, at 294–95. However, "[t]o the extent that there is general agreement that the international community has a legal duty to protect citizens from an abusive government, it stops with [the Responsibility to Protect]—and the ability for an individual state to use force to fulfill such a duty remains contingent on Security Council authorization." *Id.* at 296.

275 *See, e.g.*, Uría, *supra* note 82.

276 *See id.*; Bruce Schneier, *Hacking the Vote*, SCHNEIER ON SECURITY (Aug. 1, 2016, 6:49 AM), https://www.schneier.com/blog/archives/2016/08/hacking_the_vot.html, [http://perma.cc/4GCW-A9SE].

277 *See* Jordan Robertson, Michael Riley & Andrew Willis, *How to Hack an Election*, BLOOMBERG (Mar. 31, 2016), http://www.bloomberg.com/features/2016-how-to-hack-an-election [http://perma.cc/JDB3-8BFE] (detailing Andrés Sepúlveda's claims to have rigged Latin America elections for nearly a decade). Companies in search of state clients are also advertising "pollut[ion]" campaigns, whereby they alter internet search results and social media algorithms "to manipulate current events" and Distributed Denial of Service (DDOS) attacks to take specific sites offline. Lorenzo Franceschi-Bicchierai, *This Leaked Catalog Offers 'Weaponized Information' That Can Flood the Web*, MOTHERBOARD (Sept. 2, 2016, 10:50 AM), https://motherboard.vice.com/read/leaked-catalog-weaponized-information-twitter-aglaya [http://perma.cc/ZX9Y-YJ3K].

278 *See, e.g.*, Andrew Appel, *Security Against Election Hacking – Part 1: Software Independence*, FREEDOM TO TINKER (Aug. 17, 2016), https://freedom-to-tinker.com/2016/08/17/security-against-election-hacking-part-1-software-independence [http://perma.cc/6TET-CKKZ] (reviewing state and county election vulnerabilities); Schneier, *supra* note 276 (discussing how the results of popular

Election manipulation is just one example of how cyberspace permits an entirely new level of non-physical but nonetheless pervasive interference. Meanwhile, not only are some of the traditional obstacles to interference inapplicable in cyberspace, many of the existing deterrents are less effective.

First, the shift from physical space to the cyber realm enables states to engage in entirely new levels of invasive but nonviolent interference. States can reach into the very heart of another state's operations and steal, manipulate, or delete critical information, allowing them to obtain or compromise information on a scale previously unimaginable.

Simultaneously, many of the traditional practical obstacles to different kinds of interference are simply not applicable. Historically, influence operations required extensive intelligence, personnel, or military resources, costs that limited which states could intervene and how often they were willing to do so. That is no longer the case. States can now engage in all kinds of invasive operations without any individual ever crossing a border and at dramatically lower price points. In 2014, industry experts estimated that it would cost roughly about $10,000 for a state to develop Stuxnet-like malware.[279] More recently, an expert calculated the cost of developing and operating a new Advanced Persistent Threat—malware that can "break into any [specific] target, exfiltrate data, analyse it and produce intelligence product"—for one year to be a mere $2 million.[280]

By lowering costs, cyber lowers the barrier to entry, increasing the number of states able to engage in such interference. Certainly, electoral interference is nothing new. Dov Levin estimates that, from 1946 to 2000, either the United States or the U.S.S.R./Russia interfered in another country's elections 117 times, which roughly translates to an intervention in one of every nine competitive national-level executive

---

electronic voting machines could be manipulated); *cf.* CAITRIONA FITZGERALD, PAMELA SMITH & SUSANNAH GOODMAN, THE SECRET BALLOT AT RISK: RECOMMENDATIONS FOR PROTECTING DEMOCRACY 7 (2016), http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf [https://perma.cc/MS9C-XFQB] (proposing various solutions).

279 Dennis Fisher, *Cost of Doing APT Business Dropping*, THREATPOST (Feb. 6, 2014, 11:33 AM), https://threatpost.com/cost-of-doing-apt-business-dropping/104093 [https://perma.cc/39XS-4W3A].

280 The grugq, *Cyber: Ignore the Penetration Testers*, MEDIUM (Oct. 12, 2016), https://medium.com/@thegrugq/cyber-ignore-the-penetration-testers-900e76a49500#.adexop5g4 [http://perma.cc/ZD2K-DZ9J] (noting that this figure does not include infrastructure, personnel, or marginal costs) (alteration in original).

elections during this fifty-year period.[281] Nor is the fact that powerful states are interfering in each other's elections particularly revolutionary.[282] What is novel is that the United States and Russia are no longer the only states capable of such interference. Small states and even non-state actors may now have the resources and capacity to interfere in the affairs of others.[283]

Not only is it easier for more states to engage in more invasive cyberoperations, but traditional legal deterrents are less effective. Most physical violations of sovereignty and interventions are public. The victim state can respond immediately, and the audience of third-party states, international organizations, non-governmental organizations, and non-state actors witness the original action, observe the victim state's response, and react accordingly. Invasive cyberoperations, in contrast, can be simultaneously pervasive, destructive, and entirely secret. How is a victim state supposed to react when it does not know the perpetrator, the meaning of the act—or even that the act occurred? Finally, even if the victim state identifies the act and can reasonably attribute it to another state, it has few lawful responsive options, resulting in the state paralysis discussed earlier.[284]

In short, cyberspace undermines many of the practical and legal deterrents to interference while simultaneously promising greater payoffs. The clear implication is that cyber-enabled interference is likely to skyrocket. How should victim states respond?

C. How State Liability Might Minimize Resort to Countermeasures

Certainly, some cyber-enabled interferences will easily meet the traditional definitions for violations of state sovereignty or intervention and can be addressed under the existing law of state responsibility.[285] But states are grappling with

---

281 *See* Dov H. Levin, *Sure the U.S. and Russia Often Meddle in Foreign Elections. Does It Matter?*, WASH. POST (Sept. 7, 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/07/sure-the-u-s-and-russia-often-meddle-in-foreign-elections-does-it-matter/ [http://perma.cc/JYB4-7LYY] (noting cases where other states attempted to influence U.S. elections).

282 *Id.* (noting cases where the Soviets attempted to influence U.S. elections).

283 *See* Michael Glennon, *State-level Cybersecurity*, 171 POL'Y REV. 85 (2012) (noting the sharp increase in cyberoperations targeting a wide range of private corporations and national governments).

284 *See supra* section I.B.3.

285 *See* TALLIN MANUAL 2.0, *supra* note 46, r. 4 cmt. 11 (providing examples).

how to respond to hacks, info dumps, and other new forms of interference occurring on an unprecedented, cyber-enabled scale. For example, in the wake of an increase in "aggressive cyberespionage" targeting German politicians and a November 2016 cyberincident that caused 900,000 Germans to lose internet access, the head of Germany's foreign intelligence service warned that Russia might be interfering in Germany's elections.[286] He remarked that "cyberattacks take place which have no other purpose than to provoke political uncertainty. . . . A kind of pressure is being exercised on public discourse and democracy here, which is unacceptable."[287] Former CIA Acting Director Michael Morrell made similar statements regarding Russian interference in the 2016 U.S. general election: "It is an attack on our very democracy. It's an attack on who we are as a people. A foreign government messing around in our elections is . . . the political equivalent of 9/11."[288]

Recent cyberoperations have raised one of the perennial questions associated with new technology: is it enough to apply the existing rules, or is there something unique about the traits or effects of the new technology that requires new law?[289] Many of the rules developed in the physical world are not easily translated to cyberspace.[290] Clearly, the prohibitions on violating another state's sovereignty or engaging in interventions do not sufficiently address problems that arise in the cyber domain: despite the havoc it caused, the DNC hack alone might not qualify as a violation of U.S. sovereignty, because nothing was damaged, nor as a prohibited intervention, because the dissemination of hacked private emails was not sufficiently coercive.

Accordingly, there is an understandable desire to stretch existing terms regarding internationally wrongful acts to these

---

286 *See* Melissa Eddy, *After Cyberattacks, Germany Fears Russia May Disrupt Vote*, N.Y. TIMES, Dec. 9, 2016, at A6.

287 *Id.*

288 Morell & Kelly, *supra* note 12.

289 *Cf.* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL FORUM 207, 215–16 (arguing against developing increasingly specialized rules in response to new technologies).

290 *Cf.* Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123 (2013) (noting that states have responded to the legal confusion of cyberspace by attempting to apply laws developed for the physical world, with mixed success); Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS, *supra* note 20, at 129, 129–32, 142–58 (discussing the benefits and drawbacks with reasoning by analogy in cyberspace).

new activities, both to clarify their wrongfulness and justify the use of countermeasures. Some are arguing for expanding the definition of coercion to encompass activities like the DNC hack, either by altering or doing away with the coercion requirement entirely.[291] Duncan Hollis suggests that the intentional nature of the leak and the timing, which "clearly sought to maximize attention (and corresponding impacts) on the U.S. domestic political campaign process," warrants characterizing it as intervention.[292] Schmitt argues that the "sounder" understanding of the DNC hack is that it was coercive because "the cyber operations manipulated the process of elections and therefore caused them to unfold in a way that they otherwise would not have."[293]

However, many of these proposed solutions would transmute many of today's routine and minor interferences into prohibited interventions—with undesirable side effects. Not only might a lowered threshold for prohibited coercion deter some entities from engaging in humanitarian activities,[294] actions that states are currently expected to let go unpunished in the interest of preserving international peace would become internationally wrongful acts, justifying state resort to escalatory unilateral countermeasures. Similar problems would attend a more expansive definition of state sovereignty. As Walton has noted, "[A] definition of sovereignty that is too broad might inadvertently cover a whole host of cross-border intrusions accepted in an interconnected world, such as the extraterritorial effects of a state's telecommunications, industrial, monetary, and environmental activities."[295] Nor would expanding the universe of what constitutes unlawful interference necessarily

---

291 *See, e.g.*, Ido Kilovaty, *The Democratic National Committee Hack: Information as Interference*, JUST SECURITY (Aug. 1, 2016, 10:53 AM), https://www.justsecurity.org/32206/democratic-national-committee-hack-information-interference [http://perma.cc/UN76-GE4W] (proposing a version of intervention defined by the content, intent, and intrusiveness of the cyberoperation); Travis Sharp, *Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony*, J. STRATEGIC STUD. 4 (2017), http://www.tandfonline.com/eprint/yyT9WTdq7WBsdcPXQHhh/full [http://perma.cc/RV2A-C4HB] (arguing that even secret cyberoperations could be considered coercive to the extent they impose costs and destabilize an opponent's leadership).

292 Duncan Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, OPINIO JURIS (July 25, 2016, 3:02 PM), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention [http://perma.cc/D6G8-NFCZ].

293 Schmitt, *supra* note 180, at 8.

294 *See* Hathaway, *supra* note 50, at 49 (explaining that an expansive norm of non-interference might negatively affect state funding for humanitarian non-governmental organizations).

295 Walton, *supra* note 17, at 1477.

create more options for a victim state. As noted above, practical and legal limitations on the use of countermeasures in response to cyberoperations strictly curtail their utility.[296]

Instead of expanding the already-ambiguous scope of unlawful interferences to cover new kinds of invasive cyberoperations, victim states might instead take the less dramatic—but possibly more effective—option of claiming compensation for an international cybertort. Although such a claim would not address all of the harms associated with a politically-motivated interference, it will allow the victim state to name and shame the perpetrator and possibly recover compensation without the risk of creating problematic precedent, encouraging conflict escalation, or becoming itself responsible for an internationally wrongful act.[297]

* * * * *

The prior two Parts have drawn on fundamental principles from tort law and international law to construct a more comprehensive state accountability regime for different kinds of harmful actions in cyberspace, grounded in both state liability for acts with injurious consequences and state responsibility for internationally wrongful acts. The next Part considers how best to develop these accountability regimes.

IV
A COMPREHENSIVE SYSTEM OF STATE ACCOUNTABILITY IN CYBERSPACE

This Article's proposed categories and associated accountability regimes could be immediately incorporated within the existing international enforcement mechanisms. Namely, states could label harmful cyberoperations international cybertorts and demand compensation through formal or informal channels.

---

296 *See supra* section I.B.2.

297 Should international law evolve to encompass a more liberal understanding of the coercion element for cyber-enabled interventions, there is good reason to limit any such development to cyberspace. It is worth reiterating that the scope of the prohibition on intervention in the physical world is still unclear and evolving; mixing in new practices developed in cyberspace risks further muddying the waters. The fact that rules developed in the physical space do not apply well in cyberspace suggests that the reverse might be true. To avoid creating inappropriate precedent, cyber-enabled unlawful interferences with no physical effects should be distinguished from physical interferences. Doing so allows for the development of a cyber-specific countermeasures regime under the law of state responsibility, without impacting the equilibrium struck by the U.N. Charter and existing law of countermeasures.

That being acknowledged, it would be far preferable if states also create an independent institution with the expertise and investigative resources to impartially assess state accountability in cyberspace, the flexibility to adapt to changing technologies, and the enforcement authority to decrease the likelihood that victim states resort to inappropriate and potentially escalatory self-help. An institution would also contribute to the considered and comprehensive development of the international law of cyberspace, as its determinations would bridge the gap between positivist treaty law and the unhurried development of a customary international law of cyberspace.

A. State Interest in Developing the Law

Notwithstanding differing opinions on how best to do so, most agree that states must play a central role in developing the law of cyberspace.[298] To this end, states have produced and published domestic cyber policies,[299] engaged in confidence-building measures, signed bilateral and multilateral non-binding political agreements regarding state behavior in cyberspace, and negotiated and ratified the Convention on Cybercrime.[300]

States have myriad reasons to continue clarifying the law of cyberspace. In 2015, cyber threats were identified as the international community's top security threat,[301] and President Obama declared the threat of cyber warfare a national emergency.[302] Aside from the obvious national security implications, developing the law of cyberspace is vital to growing the global digital economy.[303] In listing problems associated with the lack of shared peacetime norms of state behavior in cyber-

---

298 *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 347 (2015) (noting that national governments have "decidedly veto[ed] an all-private governance model for cyber . . . [and] show no willingness to abandon the field of Internet and cyber governance . . .").

299 *See, e.g.*, UNITED KINGDOM, NATIONAL CYBER SECURITY STRATEGY 2016–2021 (2016); U.S. DEP'T OF DEFENSE, *supra* note 185; U.S. DEP'T OF STATE, DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY (2016) [hereinafter U.S. DEP'T STATE POLICY].

300 Convention on Cybercrime, *supra* note 9.

301 Kristen Eichensehr, *Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment*, JUST SECURITY (Mar. 6, 2015, 12:06 PM), https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment [https://perma.cc/3BGJ-ZSZB].

302 Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015), http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf [https://perma.cc/E9RK-8F8E].

303 *See* COMM'N ON ENHANCING NAT'L CYBERSEC., REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 47 (Dec. 2016).

space, U.S. cybersecurity experts on the President's Commission on Enhancing National Cybersecurity noted that "the international digital economy lacks the coherent systems necessary to effectively address cross-border malicious cyber activity. . . . The void in technical, policy, and legal conventions hampers information sharing and interoperability . . . [and] creates an opening for criminals to launch attacks and conduct other malicious cyber activity."[304] Given this, "[c]oordinated and effective international harmonization and cooperation are needed in order to realize the full economic promise of the nation and the world, and to allow for the efficient flow of information and ideas."[305] As Kristen Eichensehr has observed, "Even for those who may be skeptical of international engagement and international law or norms in general, the Commission's [economic-based] perception that international coordination is crucial should be persuasive."[306]

There have been some initial steps towards the development of international cyberspace peacetime norms.[307] In

---

304 *Id.*

305 *Id.* In the interest of ensuring "an open, fair, competitive, and secure global digital economy," these experts recommend that the United States "encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior." *Id.*

306 Kristen Eichensehr, *The Economic Incentives for International Cybersecurity Coordination*, JUST SECURITY (Dec. 6, 2016, 12:09 PM), https://www.justsecurity.org/35310/economic-incentives-international-cybersecurity-coordination [https://perma.cc/YHL7-3KRK].

307 The United States has been an active participant in this process. It originally worked to establish what is now the "global affirmation of the applicability of international law to state behavior in cyberspace," and it is currently attempting to foster "international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime." U.S. DEP'T STATE POLICY, *supra* note 299, at 12–13. These include four priority norms: (1) "[A] State should not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent of providing competitive advantages to its companies or commercial sectors"; (2) "[A] State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide service to the public"; (3) "[A] State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents" and "should not use CSIRTs to enable online activity that is intended to do harm"; and (4) "[A] State should cooperate, in a manner consistent with its domestic and international obligations, with requests for assistance from other States in investigating cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory." Egan, *supra* note 178.

The U.S. approach to developing international cybersecurity norms has been a study in what former U.S. Legal Advisor Harold Koh has called "Twenty-First-Century International Lawmaking"—namely, a combination of "nonlegal understandings," "layered cooperation," and "diplomatic law talk." Harold Hongju Koh,

2013, a fifteen-state U.N. Group of Governmental Experts (GGE) recognized the applicability of international law to states' cyberoperations, stating that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible [information and communication technology] environment."[308] In 2015, a twenty-state GGE recognized an inherent right to self-defense in cyberspace in a consensus report, as well as the applicability of the law of armed conflict's principles of humanity, necessity, proportionality, and distinction.[309] And while the 2017 GGE could not agree on a final report—due largely to disagreement about one paragraph—they made important progress towards developing cyberspace norms and principles.[310]

States are also articulating norms in the process of exploring the utility of cybersecurity confidence-building measures (CBMs) and through unilateral pronouncements.[311] In general, CBMs help minimize arms races and conflict escalation by reducing uncertainty about other states' capabilities. Proposed cyber CBMs tend to focus on information sharing, facilitating communication among stakeholders, and potential future international and domestic actions, such as commitments "to refrain from a certain activity of concern."[312] Additionally,

---

Address: Twenty-First-Century International Lawmaking, 101 GEO. L.J. ONLINE 1, 13–16 (2012).

308 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 8, U.N. Doc. A/68/98 (June 24, 2013).

309 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015).

310 *See* Arun Mohan Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (July 4, 2017, 1:51 PM), https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well [https://perma.cc/8MMK-XFG7]; *UN GGE: Quo vadis?* GENEVA DIGITAL WATCH (Geneva Internet Platform, Geneva, Switz.), June 2017, at 6.

311 In December 2013, for example, the Permanent Council of the Organization for Security and Cooperation in Europe established eleven CBMs in cyberspace; in March 2016, the Permanent Council expanded this list to sixteen. Org. for Sec. and Co-operation in Eur. [OSCE], *OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, Permanent Council, 1092nd Plenary Meeting, Decision No. 1202, (Mar. 10, 2016). The United States has also endorsed the use of CBMs. U.S. DEP'T STATE POLICY, *supra* note 299, at 15 (stating that "cyber CBMs have the potential to contribute substantially to international cyber stability" and proposing cyber-appropriate CBMs).

312 U.S. DEP'T STATE POLICY, *supra* note 299, at 15; *see also* Jack Goldsmith, *Contrarian Thoughts on Russia and the Presidential Election*, LAWFARE (Jan. 10, 2017, 11:30 AM), https://www.lawfareblog.com/contrarian-thoughts-russia-

states are building consensus around norms by publicizing their domestic policies and individual legal assessments of high-profile cyber incidents.[313] Brian Egan, former U.S. Legal Advisor to the Department of State, is one of many who has called on states to "publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent possible in international and domestic forums," which "will help give rise to more settled expectations of State behavior and thereby contribute to greater predictability and stability in cyberspace."[314]

Non-state entities are also playing a pivotal role in spurring an international conversation on these issues. One particularly influential project is the original *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the *Tallinn Manual 2.0*.[315] Although they were the product of an initiative of the NATO Cooperative Cyber Defence Centre of Excellence, the *Tallinn Manuals* are not an official NATO project nor were they intended to reflect states' views. Rather, they are a published collection of international law experts' joint reasoning and determinations regarding permissible state action in cyberspace, and while they are formally nonbinding, many of their pronouncements have been widely accepted as authorita-

---

and-presidential-election [https://perma.cc/GDE9-66VW] (arguing that technologically advanced states should be more open to "cutting a deal": joining agreements of mutual restraint, where they pledge to forego engaging in certain actions or activities in cyberspace).

There are significant obstacles, however, to creating effective confidence-building measures in cyberspace. First, there is the usual obstacle to CBMs: States are disinclined to share information about their capabilities. The United Kingdom and United States, for example, have been reluctant to share information about their offensive cyber capabilities with their NATO allies. David E. Sanger, *As Russian Hackers Attack, NATO Lacks a Clear Cyberwar Strategy*, N.Y. TIMES, June 17, 2016, at A13. Second, this is another situation where practices developed in the physical world don't translate well to the cyber realm. CBMs, which originated in the disarmament context, are usually state-based and depend on monitoring and verification mechanisms. However, cyberspace is dominated by non-state actors, and the "[a]nonymity, complexity, the intangible nature of digital systems, and the lack of knowledge about the intended use of hardware and software make any verification often not technically practicable or politically feasible." JASON HEALEY, JOHN C. MALLERY, KLARA TOTHOVA JORDAN & NATHANIEL V. YOUD, CONFIDENCE-BUILDING MEASURES IN CYBERSPACE: A MULTISTAKEHOLDER APPROACH FOR STABILITY AND SECURITY 1 (2014).

313 *See, e.g.*, U.K. NATIONAL CYBER SECURITY STRATEGY, *supra* note 299; U.S. DEP'T OF DEFENSE, *supra* note 185; U.S. DEP'T STATE POLICY, *supra* note 299.

314 Egan, *supra* note 178; *see also* BEN BUCHANAN & MICHAEL SULMEYER, HACKING CHADS: THE MOTIVATIONS, THREATS, AND EFFECTS OF ELECTORAL INSECURITY 18 (2016) ("[T]he United States should put forth a declaratory policy on the vital importance of elections, vowing to impose costs on any state that interferes with the integrity of the process.").

315 TALLINN MANUAL 2.0, *supra* note 46.

tive.[316] Where states, civil society, or scholars have disagreed with particular conclusions, the *Tallinn Manuals* have sparked broader and more informed discussions.[317]

But while states have an interest in clarifying the rules of the information superhighway, they do not want well-enforced speed limits.[318] The trick will be maintaining some leeway to speed while avoiding widespread crashes and pileups.[319]

B. Existing Implementation Mechanisms

States could promote this Article's proposals unilaterally, by explicitly alleging that another state's action constitutes an international cybertort and demanding restitution. It could even be argued that a state's failure to provide compensation or a reasonable defense would itself be an internationally wrongful act, justifying resort to countermeasures. It would be far preferable, however, for states to respond to harmful or intrusive cyberoperations—and thereby develop the relevant law—through institutional action. Compared with self-help measures, institutional responses are less escalatory and more legitimate.

Unfortunately, existing institutional responses are difficult to navigate. A state victim to cyber-enabled interventions could petition the United Nations for collective sanctions or the Security Council for an authorization for a limited use of force

---

316 As a result, the *Tallinn Manual* is often celebrated as an example of how non-state entities can have a particularly influential impact on the development of international law. *See, e.g.*, Kenneth Anderson, Daniel Reisner & Matthew Waxman, *Adapting the Law of Armed Conflict to Autonomous Weapon Systems*, 90 INT'L L. STUD. 386, 407–08 (2014); Crootof, *The Killer Robots Are Here*, *supra* note 60, at 1902.

317 The University of Texas at Austin, for example, hosted a symposium where scholars and military lawyers debated issues raised in the *Tallinn Manual 2.0*. *Events Calendar*, U. TEX. AUSTIN, https://calendar.utexas.edu/event/tallinn_manual_20_on_the_international_law_applicable_to_cyber_operations_symposium#.WdWwHGhSxPY [https://perma.cc/XV2F-AN6D].

318 The 2015 U.S. Law of War Manual has been critiqued for doing little to expand upon the public record of the U.S. understanding of the law of cyberspace, despite professing an interest in elucidation. Sean Watts, *Cyber Law Development and the United States Law of War Manual*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES, *supra* note 254, at 49, 63 ("More than simply confirmation of persistent ambiguities in the operation of the law of war in cyberspace, the ambiguities the *Manual* leaves unresolved are strong evidence of the US' comfort with these uncertainties and legal voids. . . . [T]he *Manual* indicates significant state reticence toward and even a present inclination against definitive clarity and precision in this challenging domain of state competition.").

319 In the context of international cybertorts, much of this leeway will be preserved in the term "significant harm," *see supra* subpart III.A, and by limiting state duties in cyberspace to compensation for the injuries caused by their cyberoperations, *see supra* section II.C.2.

against the perpetrator, but such petitions are unlikely to garner much support, in no small part because the main perpetrators of harmful cyberoperations are permanent members of the Security Council. Alternatively, a state victim to a harmful cyberoperation might file an ICJ suit alleging transboundary harm, violation of sovereignty, or intervention. But while the ICJ is well versed in international law, it lacks technical expertise in evaluating cyberoperations. It also has significant jurisdictional issues. The ICJ only has jurisdiction in contentious cases on the basis of state consent: states may agree to bring a specific issue before the Court by submitting a compromis,[320] or states may accept the Court's jurisdiction as generally compulsory.[321] But many powerful states have refused to accept or have withdrawn from the ICJ's compulsory jurisdiction,[322] and alleged perpetrators are unlikely to agree to submit a compromis.

Given these political and practical limitations, states often resort to self-help measures—or do nothing. But what if there were a more appropriate institutional option?

C. A New Institution

Ideally, states would create a new, independent institution with the expertise and investigative resources to impartially assess state accountability in cyberspace. This entity could be charged with fact-finding; alternatively or additionally, it might be tasked with determining state liability or responsibility for cyberoperations and granted the authority to recommend appropriate reparations to decrease the likelihood that victim states engage in inappropriate and escalatory self-help.

Determining the author of a cyberoperation is technically difficult and requires skilled forensic analysis, and the creation of an independent institution will hardly be a silver bullet for the myriad evidentiary challenges. But when compared with the alternatives—individual states, state coalitions, and the ICJ—an independent institution will be better able to recruit and retain individuals with the necessary expertise, conduct an

---

320 Statute of the International Court of Justice art. 36(1), June 26, 1945, 59 Stat. 1053, 33 U.N.T.S. 993.

321 *Id.* art. 36(2).

322 Only 72 of the 193 U.N. member states are subject to the ICJ's compulsory jurisdiction. *Declarations Recognizing the Jurisdiction of the Court as Compulsory*, INT'L CT. JUST., http://www.icj-cij.org/en/declarations [https://perma.cc/5B7J-JX8F]. Notably, four members of the Security Council—China, France, Russia, and the United States—do not currently accept compulsory jurisdiction.

unbiased investigation, and make broadly credible findings.[323] Delegating forensic tasks to an independent institution might also reduce disparities between states with different levels of domestic technological capabilities.

As there will rarely be direct evidence linking an entity to a cyberoperation or linking non-state actors to states, there will be vexing evidentiary issues to address in any case alleging state involvement in harmful cyberoperations. Both the victim state and the accused state will likely be unwilling to provide the access and information needed by an outside fact-finding entity. In many situations, the accused state will have exclusive access to critical evidence proving or disproving its connection to the cyberoperation, but regardless of whether it sponsored the act, it will be reluctant to produce such evidence for national security reasons. However, this is not an entirely new problem for international tribunals: the ICJ has developed a process for dealing with such situations that a new institution could adapt as needed.[324] Furthermore, a state bringing a

---

[323] *See also* CLARKE & KNAKE, *supra* note 104, at 252 (proposing an "International Cyber Forensics and Compliance Staff," an international organization with inspection teams to determine the origins of attacks, with the ability to place traffic monitoring equipment inside domestic networks).

[324] In international tribunals generally, the party alleging a fact has the burden of proving it. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. Rep. 14, ¶ 162 (Apr. 20). Circumstantial evidence is generally permissible (although it is often critically examined). *See* Michael P. Scharf & Margaux Day, *The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences*, 13 CHI. J. INT'L L. 123, 147 (2012) (analyzing jurisprudence from the ICJ, the Permanent Court of Arbitration, the Eritrea-Ethiopia Claims Commission, and the NAFTA Claims Tribunal). In situations where a claim depends on evidence in the sole possession of the accused state, the ICJ has sometimes held that the burden of proof shifts to that state. Ahmadou Sadio Diallo (Guinea v. Dem. Rep. Congo), Judgment, Merits 2012 I.C.J. Rep. 324, ¶ 55 (June 19); Gangaram Panday v. Suriname, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R., (ser. C) No. 16, ¶ 49 (Jan. 21, 1994). More often, rather than shifting the burden of proof or making formal adverse findings of fact, *see* Central Front (Eri. v. Eth.), 26 R.I.A.A. 115, 117 (Eri.-Eth. Claims Comm'n 2004) (reading negative inferences of fact against a state for failing to produce evidence), the ICJ has instead used nonproduction of evidence "as a license to resort liberally to circumstantial evidence where direct evidence would otherwise be preferred," Scharf & Day, *supra* at 128. In its 1949 *Corfu Channel* decision, the ICJ determined that, in cases where key evidence was in the possession of the accused state, the accusing state would enjoy "a more liberal recourse to inferences of fact and circumstantial evidence," provided there was no room for reasonable doubt. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, ¶ 47 (Apr. 9). In 2007, the Court revisited this evidentiary problem in the *Bosnian Genocide* case. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43 (Feb. 26). It relied on circumstantial evidence to reach a legal conclusion regarding Serbia's failure to prevent atrocities, but disregarded such evidence with regard to the claim that Serbia intended to commit genocide. (This may be because, with re-

claim and alleging improper conduct might be more willing to provide supporting evidence to gain the legitimacy that would attend an independent assessment of that information.

An independent institution might also be granted the power to issue binding decisions regarding appropriate reparations for significantly harmful or intrusive cyberoperations. It might even assign punitive damages, both to sanction past violations and serve as a non-escalatory deterrent, or proscribe permissible individual or collective countermeasures. This would fit well with the existing state responsibility regime, which charges states to first attempt to resolve disputes in tribunals and to refrain from engaging in countermeasures while a dispute is pending. A new institution might also avoid the jurisdictional problems of the ICJ: states invested in developing the law of cyberspace but concerned about broad waivers of sovereign immunity might be more willing to waive their immunity to suit and accept the limited jurisdiction of a specialized tribunal.

The creation of an independent international institution with specialized investigative, adjudicative, and norm-building capabilities is hardly a novel suggestion. The International Atomic Energy Agency is a well-respected organization that investigates and verifies state usage of lawful nuclear technologies. The American-Mexican Claims Commission, the U.N. Compensation Commission, the Iran-United States Claims Tribunal, and even the World Trade Organization might all be considered precedents.[325] These and similar institutions deter states from engaging in self-help, minimize the coordination issues of collective action, solve the jurisdictional problems of other existing institutional options, and proscribe appropriate sanctions.

---

gard to the latter claim, Serbia submitted direct evidence in support of its defense that it did not meet the intent requirement for the crime of genocide. Scharf & Day, *supra* at 143.) As a general rule, the ICJ "will permit liberal reliance on circumstantial evidence so long as two conditions are met: (1) the direct evidence is under the exclusive control of the opposing party; and (2) the circumstantial evidence does not contradict any available direct evidence or accepted facts." *Id.* at 131.

325 Relatedly, international investment tribunals are increasingly contributing to the development of relevant customary international law, with the full support of litigating states. *See* W. Michael Reisman, *Canute Confronts the Tide: State Versus Tribunals and the Evolution of the Minimum Standard in Customary International Law*, 30 ICSID REV. 616 (2015).

D. A Preferable Means of Legal Evolution

In the course of evaluating claims, a new institution would necessarily have to address novel questions of law, such as what duties states owe other states in cyberspace.[326] This approach to developing a law of cyberspace is far preferable to awaiting the evolution of a law of cyberspace via the more traditional sources of international law, namely, a treaty on state accountability in cyberspace or customary cyber international law.[327] Both treaty law and customary international law are ill-suited to developing state accountability for cyberoperations, underscoring the utility of creating an independent institution.

1. *The Unlikelihood of a Comprehensive Cybersecurity Treaty*

Many consider treaties—written agreements between two or more states[328]—to be the gold standard of international law. In contrast to other sources of international law, treaties are written documents describing legal rights and obligations of state parties to which states explicitly consent to be bound. Given this backdrop presumption, many hope that building international consensus around norms of state behavior in cyberspace may eventually lead to the codification of these norms in a broad, multilateral cybersecurity treaty.[329]

For a variety of reasons, however, a constitutive cybersecurity treaty may not be possible, especially if it attempts to regulate state conduct.[330] At the most basic level, there are few cyber-related subjects that permit mutually beneficial deals for states with differing technological capabilities, differing vulnerabilities, and differing beliefs about the appropriate amount of

---

326 *See supra* section II.C.2.

327 Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 10531, 33 U.N.T.S. 993.

328 Vienna Convention on the Law of Treaties art. 2, May 23, 1969, 1155 U.N.T.S. 331.

329 *See, e.g.*, CLARKE & KNAKE, *supra* note 104, at 250 (advocating for a cyber war convention); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 425 (2011) (describing the treaty process as "the ideal forum" for designing rules governing state conduct in cyberspace).

330 *See, e.g.*, GOLDSMITH, *supra* note 193 (discussing how a lack of mutual interest, willingness to make concessions to gain reciprocal benefits, and verification issues block the realization of a global cybersecurity treaty); 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) (arguing that the very nature of cyber-attacks will slow negotiations and enforcement of new international agreements restricting cyber-warfare).

governmental control over the internet or the dangers posed by free speech.

Indeed, not only do states desire to regulate different activities in cyberspace, many states see others' proposed norms as being antithetical to their own concerns. Jack Goldsmith has observed, "[T]here are deep and fundamental clashes not only over what practices should be outlawed but also and more broadly over what the problem is."[331] As an example, he discusses how the United States is promoting a norm against attacking civilian targets in part because it would disproportionately serve U.S. interests, given U.S. dependence on civilian networks, poor cybersecurity practices, and the fact that it already rarely attacks other states' civilian networks. Meanwhile, not only are Chinese civilian networks more secure than those in the United States, the Chinese military is not nearly as dependent on them. Why would China give up this potential military advantage in support of a norm against targeting civilians, Goldsmith questions, without gaining anything in return?[332] He concludes that "[t]he distributional consequences of any such agreement may be such that some nations will be willing to risk the threats to infrastructures from non-cooperation because the threats fall asymmetrically on their adversaries."[333] Meanwhile, China has repeatedly failed to garner widespread support for its proposals recognizing states' "cyber sovereignty"—the concept that state sovereignty justifies multi*lateral* internet governance—because this is commonly perceived to be at odds with Western visions of internet freedom and U.S. interests in preserving multi*stakeholder* internet governance.

There are also significant enforcement issues: Even assuming that states manage to negotiate a broad cybersecurity treaty with relatively narrowly-tailored terms that limit opportunities for creative interpretations,[334] how will state compliance with those terms be verified? In short, a constitutive

---

331 GOLDSMITH, *supra* note 193, at 4.

332 *Id.* at 5.

333 *Id.* at 6.

334 GOLDSMITH, *supra* note 193, at 6–7 ("[T]he cybersecurity context is and will remain bedeviled by two types of definitional difficulty. The first arises from the nature of the activity itself, which makes precise definitions of weapons, effects, and targets difficult. . . . [Second, w]hen nations disagree sharply over the matter to be regulated, they tend to agree (if at all) in vague generalities that are not terribly useful for fostering true cooperation."); *see also* Crootof, *Killer Robots Are Here*, *supra* note 60, at 1888–89 (discussing the importance of clear and narrowly tailored prohibitions to the effectiveness of a regulatory treaty).

cybersecurity treaty is unlikely to be negotiated—and if one is, it is not likely to be effective.[335]

Not only might it be impossible to negotiate or monitor an effective constitutive cybersecurity treaty, it is probably not an ideal means of developing the international law of cyberspace.[336] One of the primary strengths of a constitutive multilateral treaty is its stability, which justifies state investment during the negotiation and drafting process. However, all treaties risk becoming outdated as times and norms change—and law regulating new technology is particularly susceptible to early obsolescence. Instead of defaulting to the presumption that treaty law is superior, it is worth considering the relative benefits of other sources of international law.

2. *The Difficulty with Developing Customary International Cyber Law*

Customary international law "is recognized as existing when states generally engage in specific actions (the 'state practice' requirement) and accept that those actions are obligatory or permitted (the '*opinio juris sive necessitatis*' element)."[337] In short, "a rule of customary international law is authoritative because states generally abide by it in the belief that it is law."[338] While customary international law has been critiqued for lacking the clarity of written law, that indefiniteness is a strength—it is flexible and responsive to change, especially technological change. Accordingly, it may be preferable that the international law of cyberspace be grounded in customary international law rather than a constitutive treaty.[339]

However, there is one significant drawback to awaiting the development of customary international cyber law: namely, cyber-specific customary international law is unlikely to de-

---

335 Limited or bilateral cybersecurity treaties, however, may well be useful in some contexts, such as in the development of confidence-building measures.

336 This is contrary to what my co-authors and I have argued in the past. Hathaway et al., *supra* note 77, at 880–84.

337 Crootof, *Change Without Consent*, *supra* note 120, at 242.

338 *Id.* While scholars, practitioners, and judges tend to favor the *lex scripta* of treaty law over customary international law for various functional reasons, as a matter of doctrine the two sources of international law are co-equal. *Id.* at 285 n.274 (citing sources).

339 It is important to distinguish between simply applying existing customary international law to cyberspace and identifying the development of cyber-specific customary international law. The former considers norms developed in the physical world and attempts to determine how they operate in cyberspace; the latter would examine norms that develop based on state practice in cyberspace.

velop organically in the near future. Evidence of state practice is a fundamental requirement to the formation of customary international law.[340] Although cyber-based technologies foster the speedy development of customary international law generally by increasing the number of state interactions and facilitating the dissemination of information,[341] state practice in cyberspace is largely hidden. There simply are not enough examples to establish that states reliably act in a certain way in the belief that those actions are permitted or required by law. The few examples of state practice that come to light are the exceptions and the mistakes, and it would be imprudent to ground a governance regime on such sporadic and limited evidence.

3. *The Benefits of Institutional Legal Development*

An institution charged with developing the law of cyberspace bridges the gap between difficult-to-obtain positivist treaty law and the unhurried development of a customary international cyber law. It is a Goldilocks solution: institutional decisions and reports will have the authority and clarity of written law while maintaining flexibility and responsiveness to changing technological capabilities.

An independent institution could also contribute to the proactive development of a customary international cyber law. The institutional process will force states to articulate their understandings of relevant legal obligations, which in turn will foster scholarly and practitioner debates. Additionally, by promulgating codes of conduct or best practices, an institution could increase the likelihood that the law of cyberspace develops in a cohesive, flexible manner.

---

340 I subscribe to the traditional understanding of customary international law, which requires both a state practice and *opinio juris* element. Some have argued, however, that "modern" customary international law can be established based on evidence of *opinio juris* alone. Bin Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law?*, 5 INDIAN J. INT'L L. 23, 45 (1965), *reprinted in* INTERNATIONAL LAW: TEACHING AND PRACTICE 237, 260 (Bin Cheng ed., 1982) (arguing that "[i]nternational customary law requires only one single constitutive element, namely, the *opinio juris* of States."). For incisive critiques of this proposition, see, for example, Curtis A. Bradley & Jack L. Goldsmith, *Customary International Law As Federal Common Law: A Critique of the Modern Position*, 110 HARV. L. REV. 815, 839–40 (1997); Bruno Simma & Philip Alston, *The Sources of Human Rights Law: Custom, Jus Cogens, and General Principles*, 12 AUSTL. Y.B. INT'L L. 82, 83 (1989).

341 Crootof, *Change Without Consent*, *supra* note 120, at 245–47.

CONCLUSION

New technology often exposes gaps and vagueness in existing law and undermines foundational assumptions and justifications of legal regimes[342]—and cyberspace is no exception. Quite the contrary. Cyberspace is a particularly bewildering arena: its infrastructure is shared by civilians and militaries, governments and businesses; cyberoperations occur and must be rebuffed at super-human speeds; non-state actors can be equally—if not more—powerful than some states; and it can be difficult to identify transgressors, both because the source of cyberoperations can be masked and because states often operate through non-state actors. As a result, there is substantial normative confusion, as legal rules made for the physical world map do not always map well onto the cyber domain. Given this confusion, states have a vested interest in clarifying the international laws of cyberspace, both to know what actions they may lawfully take and how they may lawfully respond to other states' actions.

This Article draws on tort law and international law principles to construct a comprehensive system of state accountability in cyberspace, where states are both liable for their lawful but harmful acts and responsible for their wrongful ones. Not only does recognizing international cybertorts and its attendant state liability regime permit new means of managing the harms associated with data destruction, ransomware, and cyberespionage, it minimizes the likelihood that victim states will resort to escalatory self-help measures, increases the chance that those harmed by cyberoperations will be compensated, and preserves a bounded grey zone for state experimentation.

342 Lyria Bennett Moses, *Why Have a Theory of Law and Technological Change?*, 8 MINN. J.L. SCI. & TECH. 589, 595 (2007).