THE YALE LAW JOURNAL

BEATRICE A. WALTON

Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law

ABSTRACT. Low-intensity state-sponsored cyber attacks exist within a "gap" in public international law. Falling short of the definitions of use of force and intervention, these attacks are not clearly governed by international law. Some scholars have sought to stretch established international legal categories to resolve this problem, while others have suggested new treaty regimes for cyberspace altogether. I suggest an alternative: liability for the duty to prevent and redress transboundary harms. By examining the origins of this duty, this Note identifies how liability for the duty to prevent and redress transboundary harms might apply for low-intensity cyber attacks, an increasingly common and destructive category of attacks.

AUTHOR. Yale Law School, J.D., expected 2018; University of Cambridge, M.Phil., 2015; Harvard College, A.B., 2014. I am sgrateful to Professor Oona Hathaway and Professor Harold Koh for their support and guidance throughout the writing of this piece. I would also like to offer sincere thanks to S.J. Calum Agnew, Rebecca Crootof, and Asaf Lubin, without whom this project would have never gotten off the ground. Thank you to Joe Falvey and the *Yale Law Journal* Notes Committee, Ido Kilovaty, and Professor Jack Goldsmith, all of whom provided helpful comments, insights, and suggestions. Finally, I would like to express my deepest appreciation for the host of generous mentors who have guided me over the years. All errors are mine alone.

NOTE CONTENTS

INTRODUCTION

On November 24, 2014, a menacing red skull flashed on every employee's screen at Sony Pictures Entertainment's headquarters in Culver City, California. The attackers, calling themselves the "Guardians of Peace," scrubbed more than one hundred terabytes of Sony's data and leaked thousands of confidential documents.[1] The attackers threatened to release more documents if Sony did not stop the release of *The Interview*, Sony's newest political-satirical film on North Korea, and made clear their intention to cause further harm and even violence.[2] In the end, many theaters caved to the attackers' demands, refusing to screen the film—but not before the attacks resulted in tens of millions of dollars in damage,[3] including the destruction of Sony data systems,[4] the corruption of thousands of computers,[5] the loss of millions of dollars in revenues,[6] and leaked trade secrets.[7]

In the aftermath of the attack, the U.S. government made an unprecedented accusation, officially attributing the Sony attack to the government of North

1. *See* 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/ZE2Q-MM5H].

2. *See* Catherine Shoard, *Sony Hack: The Plot To Kill The Interview–a Timeline So Far*, GUARDIAN (Dec. 18, 2014, 6:35 PM), http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline [http://perma.cc/8T2Y-SDNT].

3. *See* Lianna Brinded, *The Interview Tipped To Cost Sony Pictures $200m Following Hack and Cancellation*, INT'L BUS. TIMES (Dec. 18, 2014, 4:40 PM), http://www.ibtimes.co.uk/interview-tipped-cost-sony-pictures-200m-total-following-hack-cancellation-1480157 [http://perma.cc/EJ8U-XT9B]. While the total damage to Sony is difficult to calculate, Sony has indicated that the attacks cost the company at least $15 million. *See* Ryan Faughnder, *Sony Says Studio Hack Cost It $15 Million in Fiscal Third Quarter*, L.A. TIMES (Feb. 4, 2015, 11:07 AM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-cost-20150204-story.html [http://perma.cc/Q8S6-66XS]; Andrea Peterson, *Why It's So Hard To Calculate the Cost of the Sony Pictures Hack*, WASH. POST (Dec. 5, 2014), http://www.washingtonpost.com/news/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack [http://perma.cc/S7RT-ZLNC].

4. *See* Amanda Hess, *Inside the Sony Hack*, SLATE (Nov. 22, 2015, 8:25 PM), http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html [http://perma.cc/8VYZ-XCMA].

5. *See* Press Release, Fed. Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [http://perma.cc/4ZV4-BNSD].

6. *See* Brinded, *supra* note 3.

7. *See* Lisa Richwine, *Cyber Attack Could Cost Sony Studio as Much as $100 Million*, REUTERS (Dec. 9, 2014, 5:58 PM), http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209 [http://perma.cc/72GJ-C37Z].

Korea.[8] After an FBI investigation that linked the attack's code, infrastructure, and overall design to previous attacks that were believed to have been carried out by North Korea,[9] the State Department officially condemned North Korea on December 19, 2014.[10] In a special press release, President Obama vowed that the United States would respond proportionally in the arena of its choosing.[11]

International legal and technology experts have since hotly debated the attribution of the Sony attack. Some have claimed that the United States misattributed or prematurely attributed the attack to North Korea.[12] Others have noted that the United States's actions could set a dangerous precedent.[13] In any case, observers recognize that the United States's response was a key example—now one of a steadily growing number[14]—of a state officially accusing another of a cyber attack.[15] Yet even if attribution is possible, a more pressing question for international law emerges: what international law has North Korea violated by committing this attack?

---

8. *See* Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html [http://perma.cc/742A-8GCY] (noting that this was "the first time that the United States has openly laid blame on a foreign government for a destructive cyber attack against an American corporation").

9. *See* Press Release, Fed. Bureau of Investigation, *supra* note 5. For examples of techniques relied upon by the U.S. government when tracing attacks, see *APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT (2013), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-083.pdf [http://perma.cc/V294-8BXB].

10. *See* Press Release, John Kerry, Sec'y of State, U.S. Dep't of State, Condemning Cyber-Attacks by North Korea (Dec. 19, 2014), http://www.state.gov/secretary/remarks/2014/12/235444.htm [http://perma.cc/J9JK-5PRS].

11. *See* President Barack Obama, *Remarks by the President in Year-End Press Conference*, WHITE HOUSE (Dec. 19, 2014), http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference [http://perma.cc/Y8PF-PPQY].

12. *See, e.g.*, Kim Zetter, *Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy*, WIRED (Jan. 8, 2015, 4:53 PM), http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy [http://perma.cc/43RF-ECJ9].

13. *See, e.g.*, Robert M. Lee, *The Feds Got the Sony Hack Right, but the Way They're Framing It Is Dangerous*, WIRED (Jan. 10, 2015, 6:30 AM), http://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous [http://perma.cc/D6D9-B8Y3].

14. For example, the U.S. government has recently accused Russia of interfering in the U.S. elections. *See* David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks To Influence Elections*, N.Y. TIMES (Oct. 7, 2016), http://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html [http://perma.cc/PSP6-747U].

15. *See, e.g.*, Herb Lin, *Learning from the Attack Against Sony*, LAWFARE (Jan. 23, 2015, 10:38 AM), http://www.lawfareblog.com/learning-attack-against-sony [http://perma.cc/UTH9-Z4MD]; Nakashima, *supra* note 8.

As surprising as it may seem, the traditional international legal perspective seems to answer "none."[16] Despite the increasingly common and destructive nature of state-sponsored cyber attacks,[17] it is difficult to locate the precise source of illegality for these "low-intensity" cyber attacks.[18] In the language of the *Draft Articles on State Responsibility*, states are only responsible for acts attributable to the state that are "wrongful" under international law.[19] Low-intensity state-sponsored cyber attacks do not fit this bill. Scholars have recognized this "gap" for low-intensity cyber attacks and sought solutions. Some have tried to broaden current international legal categories of impermissible conduct to cover these attacks.[20] Others have declared that a new treaty or legal regime is needed before international law can render low-intensity attacks wrongful.[21] Neither approach has proved satisfactory thus far.

This Note proposes an important theoretical and practical alternative that derives from a preexisting but underutilized source of international law: liability for transboundary harm. Liability in international law is a complicated, controversial, and often misunderstood concept that has developed separately from, but directly feeds into, the customary international legal regime of state responsibility. Liability does not emerge from a violation of international law

16. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 820 (2012) ("Some have referred to these and similar attacks as 'cyber-warfare,' suggesting that the law of war might apply. Yet the attacks look little like the armed conflict that the law of war traditionally regulates."); Michael Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SECURITY L. 245, 246 (2012) ("Cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict . . . . Moreover, massive attacks can be launched by a single individual or by a group that is organized entirely on-line. This is in sharp contrast to traditional warfare . . . .").

17. *See* Sean Watts, *Low Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 249-50 (Jens David Ohlin et al. eds., 2015).

18. Under the doctrine of state responsibility, states are responsible for "wrongful" acts that are (a) attributable to the state and (b) breaches of an international obligation. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 2, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 68 (2001) [hereinafter Draft Articles on State Responsibility].

19. *Id.* art. 2, at 68.

20. *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129-33 (1999).

21. *See, e.g.*, Rebecca Crootof, Cyberinterference (2016) (unpublished manuscript) (on file with author). For an analysis of why comprehensive treaty regimes are unlikely in cyberspace, see Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INST. (Mar. 9, 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf [http://perma.cc/Y8QW-WRX7].

per se, which would constitute wrongfulness (or even give rise to international criminal responsibility), but rather, simply from an act of *harm*.

In particular, liability in international law derives from the customary duty to prevent and redress transboundary harm. This duty is most familiar in the environmental realm,[22] despite its roots in and application to a broader range of legal issues.[23] International liability for a violation of this duty is triggered by the "transboundary movement of . . . harmful effects" above a certain level of severity not traditionally tolerated,[24] and involving a causal relationship between the damage caused and the activity causing it.[25]

To make the case for applying this liability approach to low-intensity state-sponsored cyber attacks, this Note proceeds in four Parts. Part I begins by explaining why low-intensity cyber attacks appear to escape regulation under existing international legal obligations. Part II next examines the origins of the duty to prevent and redress transboundary harm, which forms the basis of international liability, and the complex relationship between liability and the doctrine of state responsibility. Part III applies liability for this duty to low-intensity, state-sponsored cyber attacks. Part IV then turns to the three key benefits of a liability approach for cyber attacks: (1) pragmatic appeal to states' interests and emphasis on the duty to redress harms, (2) clarification of the literature on due diligence and countermeasures in international law, and (3)

---

22. *See infra* Section II.A.

23. For example, liability for transboundary harm has been pursued in the context of damages caused by space objects and by misfired weapons and mines. The International Law Commission (ILC) contemplated applying liability for transboundary harm to a broader range of activities in its work in its work on "liability for injurious consequences arising out of acts not prohibited by international law." *See infra* text accompanying notes 106-114.

24. XUE HANQIN, TRANSBOUNDARY DAMAGE IN INTERNATIONAL LAW 8 (2003) ("To be legally relevant, damage should be at least 'greater than the mere nuisance or insignificant harm which is not normally tolerated.'") (quoting Int'l Law Comm'n, Sixth Report on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited By International Law, arts. 2(b), 2(e), U.N. Doc. A/CN.4/428 (Mar. 15, 1990)). While Xue notes that "international law only tackles those cases where transboundary damage has reached a certain degree of severity," different thresholds of severity are required for transboundary liability "for different purposes and in different contexts." *Id.* at 7-8.

25. *See id.* at 4, 7-8. "Transboundary" refers to damages caused directly between two or more states, as well as damages that have transcended boundaries. "Harmful effects" include physical damage to persons or property, as well as intangible damages caused by economic activities. "Severity" requires a factual inquiry particular to the circumstances of each incident, given that international law generally accepts liability only for damages "greater than the mere nuisance or insignificant harm which is normally tolerated" by the international community. *Id.* at 8. "Causation" requires a proximal, though not necessarily physical, link between an activity and the ill effects produced. *Id.*

acknowledgement of duties owed to third parties. This Note ultimately proposes that liability for transboundary harm offers a fruitful approach for bringing low-intensity cyber attacks into the fold of international law.

I. THE PUZZLE OF LOW-INTENSITY STATE-SPONSORED CYBER ATTACKS

Before turning to liability for transboundary harm and how it might apply in the cyber realm, this Part describes the problems posed by low-intensity cyber attacks and why established international legal principles have proven incapable of regulating these attacks.

A. The Problem

A cyber attack is "any action taken to undermine the functions of a computer network for a political or national security purpose."[26] Low-intensity cyber attacks, specifically, encompass any of a wide range of actions taken to "alter, disrupt, deceive, degrade, or destroy" computer systems or networks resulting in destruction and coercion insufficient to amount to a use of force or intervention under international law.[27] As the latter half of this definition makes clear, defining low-intensity cyber attacks inevitably involves a discussion of what they are *not*: actions clearly governed by established international legal rules. Here, I briefly explain why low-intensity cyber attacks merit attention and why bringing law to bear on them is a worthwhile goal in the first place.

First, low-intensity cyber attacks are incredibly costly. Experts suggest that the average large U.S. company spends more than $7.7 million on preventing and responding to cyber attacks each year, a relatively high amount compared to that spent by large foreign companies.[28] Around the world, the numbers are

---

26. Hathaway et al., *supra* note 16, at 826.

27. The National Research Council defines cyber attacks as actions intending to "alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks." NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10-11 (William A. Owens et al. eds., 2009); *see* Christopher S. Yoo, *Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS, *supra* note 17, at 175; Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014, 9:29 AM), http://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea [http://perma.cc/R38E-G43Q].

28. *Cost of Cyber Crime Study: Global*, PONEMON INST. (2015), http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html [http://perma.cc/79WF

similarly startling: cyber attacks result in more than $400 billion in losses to companies each year,[29] and potentially as much as $2.1 trillion in losses by 2019.[30] While governments and private entities have dramatically boosted their cyber security in recent years, experts remain convinced that even the best security precautions remain incapable of eliminating all vulnerability to future attacks.[31] This is troubling, given that even a single vulnerability can open the door to considerable destruction; the attack on Sony, for instance, resulted in the destruction of three thousand computers and eight hundred servers.[32]

Moreover, low-intensity cyber attacks are incredibly common. While much scholarly attention has focused on the threat of major cyber attacks that border on acts of war, the most common cyber attacks fall considerably below this level. In 2015, only 2.4% of all cyber attacks were conducted in the context of war or gave rise to a degree of physical damage approaching a use of force.[33] In fact, experts agree that "[f]ew, if any, cyber operations have [ever] crossed the armed attack threshold."[34] The need for legal restrictions on and remedies for cyber attacks is no less severe given the immense impact that these attacks have on personal and state property.

-8G6B]. Others suggest an even larger average cost to U.S. firms. *See* James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN (Oct. 8, 2015, 3:28 AM), http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business [http://perma.cc/PR7W-HLP4].

29. *Net Losses: Estimating the Global Cost of Cybercrime*, CTR. FOR STRATEGIC & INT'L STUD. (June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [http://perma.cc/8GQM-W5P9]; Will Yakowicz, *Companies Lose $400 Billion to Hackers Each Year*, INC. (Sept. 8, 2015), http://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html [http://perma.cc/8PN8-M2FK].

30. Steve Morgan, *Cyber Crime Costs Projected To Reach $2 Trillion by 2019*, FORBES (Jan. 17, 2016, 11:01 AM), http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019 [http://perma.cc/4FGK-5FD4]. However, these figures remain rough estimates because the costs that result from privacy infringements and intellectual property losses remain difficult to calculate.

31. *See* ERIC COLE, ADVANCED PERSISTENT THREAT: UNDERSTANDING THE DANGER AND HOW TO PROTECT YOUR ORGANIZATION 27 (2013).

32. *See* Steve Kroft, *The Attack on Sony*, CBS (Apr. 12, 2015), http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes [http://perma.cc/XXS2-ZGSB]. Another attack, which took place in 2012, was believed to have been carried out by Iran on Saudi Arabia's national oil company, Aramco, destroyed thirty thousand computers. *See id.*

33. Paulo Passeri, *2015 Cyber Attacks Statistics*, HACKMAGEDDON (Jan. 11, 2016), http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics [http://perma.cc/WB5W-8USZ].

34. Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 698 (2014).

Third, even if it were possible to expand existing categories of law to encompass low-intensity cyber attacks, doing so could create havoc in other areas of law. As the next Section and Part IV explain, expanding the concepts of nonintervention and sovereignty in international law could result in problems for NGOs and other supporters of human rights who engage in political activities abroad. Such an expansion would also complicate our understandings of which routine cross-border infringements constitute violations of international law.[35]

Depending on how existing bodies of international law are broadened, states might also either lose the right to respond "in kind" to low-intensity cyber attacks, or conversely, gain the right to respond with disproportionately numerous counterattacks.[36] But such measures may be unsustainable, as escalations are likely to mount over time if states are permitted to respond to low-intensity attacks without restriction. For instance, after the Sony attack, it appears likely that a portion of North Korea's internet was temporarily knocked offline although it is unclear who mounted the response.[37] Like the initial Sony hack itself, such counterattacks are, by their nature, difficult to control. Subsequent miscalculations, human coding error, and varying perceptions of the damage can lead a response to cause even greater destruction and more severe legal consequences than was initially intended.[38] Nevertheless, the alternative—

35. *See* Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, *in* 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: PROCEEDINGS 39, 43-44 (P. Brangetto et al. eds., 2014), http://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2014.pdf [http://perma.cc/9LS8-3B6E].

36. For countermeasures (the appropriate term if the underlying attack is considered illegal, and if the response to it involves methods that too would be considered illegal if not in this context), see Draft Articles on State Responsibility, *supra* note 18, art. 49, at 328-33. For retorsions (the appropriate term if the response involves only unfriendly, but not illegal, actions), see Thomas Giegerich, *Retorsion*, *in* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (Mar. 2011), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983 [http://perma.cc/JZT7-CV6P].

37. Martin Fackler, *North Korea Accuses U.S. of Staging Internet Failure*, N.Y. TIMES (Dec. 27, 2014), http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html [http://perma.cc/E6MK-DWRG].

38. *See* Angela McKay et al., *International Cyber Security Norms: Reducing Conflict in an Internet-Dependent World*, MICROSOFT 4 (2014), http://www.microsoft.com/en-us/download/details.aspx?id=45031 [http://perma.cc/5F7A-5HCM] ("Given the interconnected nature of cyberspace and the speed and nature of cyber attacks, the effects of offensive operations might be very difficult to predict and/or limit, and they could cascade to affect operations beyond the intended targets, including critical functions in the energy, communications, banking, chemical, or transportation sectors, among others. In other instances, an offensive cyber operation gone wrong could disrupt the global Internet or corrupt data at a scale that impedes key functions of the global economy. Unintended consequences of this scale could very easi-

leaving low-intensity cyber attacks unaddressed—may also have a corruptive effect on the international legal order.[39] By encouraging self-help, unfriendly action, and non-cooperation, this option has the potential to blur the fundamental boundary between peace and conflict and thereby generate heightened anxiety about future destruction.[40]

Therefore, a response to low-intensity cyber attacks is necessary, but as the next Section explains, an adequate response is unavailable under traditional legal frameworks.

B. The Gap in International Law

In this Section, I consider a number of legal rules that lack clear application to low-intensity cyber attacks, including international law on the use of force, intervention, armed conflict, and respect for state sovereignty.

The prohibition on the use of force—which the International Court of Justice (ICJ) has declared a "cornerstone of the United Nations Charter"—is the most natural place to look for international law applicable to low-intensity cyber attacks.[41] Article 2(4) of the UN Charter proclaims, "All Members shall refrain . . . 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 Nations."[42] While the scope of Article 2(4)'s prohibition on the use of force is hotly debated,[43] the object and purpose of the UN Char-

---

ly escalate hostilities from the keyboard to kinetics, in the absence of normative limits on such behaviors.").

39. *See id.* at 4; *infra* notes 253-254 (describing how an error in the Stuxnet code led to its unintentional, albeit benign, spread to computers around the world).

40. *See* McKay et al., *supra* note 38, at 4 ("[T]he increasing development of defensive and offensive cyberspace capabilities will, in itself, promote cyber insecurity between nation states, especially without a normative framework around those capabilities. If a state, for example, shifts cybersecurity investments from civilian defense and law enforcement to offensive military capabilities, other states will react. The actions of individual nation states could exacerbate cyber insecurity regionally or globally, driving broader tensions in the international system.").

41. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 148 (Dec. 19). This prohibition is also provided for in 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).

42. U.N. Charter art. 2, ¶ 4.

43. *See* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 30 (3d ed. 2008).

ter[44] and its *travaux préparatoires*[45] support a conclusion that Article 2(4) likely refers to "armed force,"[46] or at least to incidents giving rise to significant physical damage.[47] Adapting the prohibition on the use of force to cyber attacks, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*), a NATO-commissioned study produced by an international group of experts on the legality of cyber conflicts, has relied on this traditional approach. The *Tallinn Manual* reasons that only cyber attacks of sufficient "severity," "invasiveness," and "military character" amount to uses of force.[48]

---

44. U.N. Charter, pmbl. ("We the people of the United Nations determined . . . to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest . . . have resolved to combine our efforts to accomplish these aims.").

45. U.N. Conference on Int'l Orgs., *Summary Report of Eleventh Meeting of Committee I/1*, *in* 6 DOCUMENTS OF THE CONFERENCE ON INTERNATIONAL ORGANIZATION 331, 334 (1945). The *travaux préparatoires* (meaning "preparatory works") are the official records of a negotiation.

46. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (5th ed. 1998); 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 208 (Bruno Simma et al. eds., 3d ed. 2012); Hathaway et al., *supra* note 16, at 842; *see also* Bert V. A. Röling, *The Ban on the Use of Force and the U.N. Charter*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 3 (A. Cassese ed., 1986) (finding it "obvious" that Article 2(4) refers to armed force); Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 135, 172-74 (Katharina Ziolkowski ed., 2013) (summoning multiple lines of evidence for the proposition that Article 2(4) refers to armed force, and describing actions to which Article 2(4) might apply).

47. The *travaux préparatoires* suggest that participants of the San Francisco Conference in April 1945, which culminated in a draft of the UN Charter, specifically rejected an amendment that would have included economic coercion within the scope of Article 2(4). *See* U.N. Conference on Int'l Orgs., *supra* note 45, at 334; *see* Yoo, *supra* note 27, at 178-79. In addition to rejecting such a proposal by Brazil to include economic force, the Conference also declined to take up Iran's suggestion to include political force in the prohibition. *See* Nico Schrijver, *The Ban on the Use of Force in the UN Charter*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 470-71 (Marc Weller ed., 2015). In addition, the prevailing consensus that Article 2(4) only applies to "armed force" is supported by arguments that Article 2(4) was drafted with the goal to limit unilateral recourse to specifically "armed" conflict. *See* Hathaway, *supra* note 35, at 43-44; *see also* Michael N. Schmitt, *The Use of Cyber Force and International Law*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW, *supra*, at 1110-13 (discussing negotiations concerning the use of force definition).

48. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 48-52 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. Rule 11 of the *Tallinn Manual* specifically notes that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." *Id.* at 45.

In light of the *Tallinn Manual* and a growing consensus in favor of such an "effects-based" approach,[49] low-intensity cyber attacks appear to escape prohibition under Article 2(4), because they typically fail to cause the extensive physical destruction necessary to meet the traditional definition of use of force.[50] For example, while the Sony attack resulted in the destruction of more than three-quarters of Sony's main studio computers,[51] most scholars agree that this destruction is not comparable to destruction caused by kinetic operations and therefore is beyond the scope of use of force under international law.[52]

Second, unless low-intensity cyber attacks take place within the context of a preexisting international armed conflict, they are not clearly governed by the

---

49. *See, e.g.*, OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN MILITARY OPERATIONS (2d ed., 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 459, 483 (Michael N. Schmitt & Brian T. O'Donnell eds., 1999) ("[T]he consequences are likely to be more important than the means used."); Schmitt, *supra* note 47, at 1113-16; Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace: Remarks at the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *reprinted in* 54 HARV. INT'L L.J. ONLINE 1, 4 (2012). It should be noted, however, that direct use of weapons by a state is not required to violate the prohibition, as enabling other actors to use such weapons can constitute a violation as well. *See* MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 66-67 (2014) ("In the *Nicaragua* judgment, the I.C.J. also qualified the arming and training of armed groups—not directly destructive actions—as a use of force.").

50. *See* TALLINN MANUAL, *supra* note 48, at 47.

51. *See* David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES (Jan. 2, 2015), http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html [http://perma.cc/39NM-H58G].

52. *See* Koh, *supra* note 49, at 4 ("[I]f the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."); *see also* Erki Kodar, *Computer Network Attacks in the Grey Areas of* Jus ad Bellum *and* Jus in Bello, 9 BALTIC Y.B. INT'L L. 133, 139-40 (2009); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914-15 (1999). To date, the Stuxnet attack, which destroyed nuclear centrifuges inside Iran's Natanz uranium enrichment site, remains the only cyber attack widely accepted by scholars as a potential use of force. *See, e.g.*, Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SECURITY L. 212, 220-21 (2012). While debate nevertheless surrounds the lower threshold of Article 2(4), some examples of cyber attack consequences clearly constituting force have been suggested: a nuclear plant meltdown, the opening of a dam, or even the disabling of air traffic such that planes crash. *See* Koh, *supra* note 49, at 4. For discussion of the lower bounds of the use of force threshold, particularly in the context of blockades, see Penelope Neville, *Military Sanctions Enforcement in the Absence of Express Authorization?*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW, *supra* note 47, at 279-83.

laws of armed conflict (*jus in bello*).[53] Under international law, "armed attacks," which encompass attacks involving the "most grave forms of the use of force,"[54] trigger the right of a state to self-defense under Article 51 of the UN Charter, as well as the application of *jus in bello*.[55] While some states, such as the United States, maintain that armed attacks are synonymous with mere uses of force,[56] it is clear that low-intensity cyber attacks fall short of either a use of force or an armed attack, and thus do not give rise to *jus in bello* restrictions.[57]

Third, low-intensity attacks also fail to qualify as unlawful "interventions."[58] Customary international law suggests that an intervention requires "methods of coercion"[59] "bearing on matters in which each State is permitted, by the principle of state sovereignty, to decide freely," such as its "political, eco-

---

53. *See* Crootof, *supra* note 21. The United Nations Group of Governmental Experts agreed that an armed attack in cyberspace need not require "armed" employment of weapons, as injuries to persons or damages to physical property may also meet the armed attack threshold. *See* Yoo, *supra* note 27, at 181.

54. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 91, ¶ 191 (June 27).

55. *See* U.N. Charter art. 51. Though there has been no clear agreement yet on whether such an example has taken place, scholars nevertheless agree that it is possible for a cyber attack to meet the threshold of an "armed attack" if its effects approach those of kinetic armed attack. *See* Hathaway et al., *supra* note 16, at 836-37; Kodar, *supra* note 52, at 139-40; Schmitt, *supra* note 52, at 914-15; 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, 427 (2011).

56. *See* Koh, *supra* note 49, at 7. *But see* Hathaway, *supra* note 35, at 49 ("[T]he UN Charter does not permit states to respond with force to every single illegal use of force—in particular, to those uses of force that do not arise to the "most grave" level sufficient to amount to an "armed attack" and trigger Article 51.").

57. *See* Schmitt, *supra* note 27.

58. *See Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 106, ¶ 202; G.A. Res. 2625 (XXV), at 5 (Oct. 24, 1970); G.A. Res. 2131 (XX), ¶ 2 (Dec. 21, 1965). Attacks which aim to change the outcome of an election may be more likely to constitute an intervention, as opposed to a mere low-intensity cyber attack.

59. *Oppenheim's International Law* defines "intervention" as requiring interference that is "forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention." 1 OPPENHEIM'S INTERNATIONAL LAW 432 (Robert Jennings & Arthur Watts eds., 9th ed. 2008). Put another way, intervention "aims to impose a certain conduct of consequence on a sovereign state." Philip Kunig, *Prohibition of Intervention*, *in* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. ¶ 1 (Apr. 2008), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434 [http://perma.cc/3DBK-WFTV].

nomic, social and cultural" system.[60] Low-intensity cyber attacks struggle to meet this definition because they are typically targeted at private entities, create relatively localized harms within a state, and do not impact policy matters traditionally within the *domaine réservé* of the state[61]—a necessary element of "coercion" within the definition of intervention.[62] While not every attack failing to meet the definition of the use of force falls outside of the definition of intervention, many do.[63] The prohibition on intervention applies narrowly in cyber attacks, because intervention has routinely required more than mere "interference."[64] For example, Iran's attack on the Sands Casino in 2014 resulted in more than $40 million in damage to the Las Vegas Sands Corporation from destroyed data and computer systems, yet the attack had no broader political impact.[65]

Fourth, low-intensity cyber attacks initiated by states do not constitute "cyber crime." International criminal law applies only to individual actors, not

---

60. *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. at 107-08, ¶ 205. *Nicaragua* also uses the language of "political integrity." *Id.* at 106, ¶ 202; *see* TALLINN MANUAL, *supra* note 48, r. 10, cmt. 10, at 45.

61. *See* Schmitt, *supra* note 27; Katja S. Ziegler, *Domaine Réservé*, *in* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. ¶ 1 (Apr. 2013), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398 [http://perma.cc/JR6J-NNSH]. *Oppenheim's International Law* explains that in addition to being closely linked to the concept of *domaine réservé*, the principle of non-intervention is a "corollary of every state's right to sovereignty, territorial integrity and political independence." 1 OPPENHEIM'S INTERNATIONAL LAW, *supra* note 59, at 428.

62. While coercion remains key to most scholarly conceptions of intervention, Watts notes that "[s]tates have not achieved or expressed consensus on a notion of coercion sufficient to constitute intervention," much less in the cyber context. Watts, *supra* note 17, at 270.

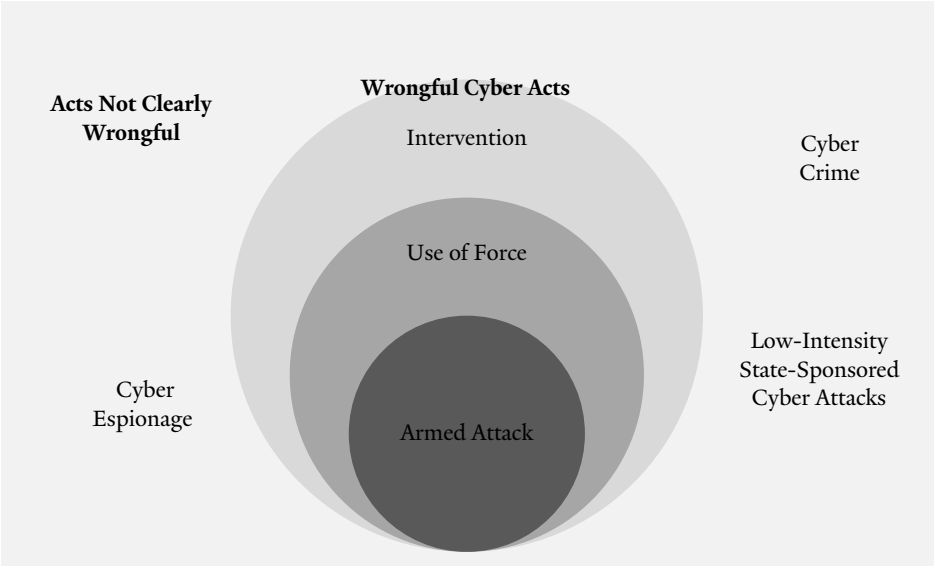
63. *See, e.g.*, Schmitt, *supra* note 27.

64. *See, e.g.*, TALLINN MANUAL, *supra* note 48, r. 10, cmt. 8, at 44-45; Schmitt, *supra* note 47, at 1113-17; Schmitt, *supra* note 27.

65. *See* Crootof, *supra* note 21; 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/UHD2-DLMZ]; *cf.* Max Kutner, *Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure*, NEWSWEEK (Mar. 30, 2016, 8:12 AM), http://www.newsweek.com/cyber-attack-rye-dam-iran-441940 [http://perma.cc/E46K-XPCS] (describing an incident in which a hacker affiliated with the Iranian government allegedly hacked a New York dam); Jordan Robertson & Michael Riley, *American Airlines, Sabre Said To Be Hit in China-Tied Hacks*, BLOOMBERG (Aug. 7, 2015, 5:00 AM), http://www.bloomberg.com/news/articles/2015-08-07/american-airlines-sabre-said-to-be-hit-in-hacks-backed-by-china [http://perma.cc/B2RM-Q8TD] (describing a series of attacks on corporations related to the U.S. travel industry that were allegedly attributable to hackers linked to China).

states, and scant international criminal law is directly applicable to low-intensity cyber attacks.[66] Nonetheless, state-sponsored cyber attacks typically remain "more advanced and dangerous" than routine cyber crimes carried out by non-state hackers.[67] For this reason, Facebook and Google notify users when they believe accounts have been targeted or compromised by an attacker suspected of "working on behalf of a nation-state,"[68] as opposed to mere individuals.

FIGURE 1.
CYBER ACTS IN INTERNATIONAL LAW



Recognizing that low-intensity state-sponsored cyber attacks fall beyond the bounds of traditional international law, some scholars have recently at-

66. *See* Crootof, *supra* note 21, at 2 ("Assuming that they were state-sponsored, they weren't cybercrime.").

67. *Id.* at 4 (quoting Brian Barrett, *Facebook Now Warns Users of State-Sponsored Attacks*, WIRED (Oct. 19, 2015, 11:28 AM), http://www.wired.com/2015/10/facebook-now-warns-users-of-state-sponsored-attacks [http://perma.cc/L5MQ-EKGR]).

68. *Notifications for Targeted Attacks*, FACEBOOK (Oct. 16, 2015, 4:36 PM), http://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766 [http://perma.cc/5RZA-9K2U] (explaining Facebook's policy of notifying users of attacks by persons "suspected of working on behalf of a nation-state").

tempted—albeit with limited success—to apply broader customary international law principles to the low-intensity cyber arena. After all, within the doctrine of state responsibility, state action is wrongful when the conduct is "attributable to the State under international law" and "[c]onstitutes a breach of an international obligation of the State."[69] Finding a source of such breached obligations would not only deem low-intensity cyber attacks wrongful, but would also entitle injured states to seek cessation of the offense, reparation, assurances of non-repetition, and perhaps even countermeasures if the offense continues.[70] These approaches, however, have struggled to proscribe low-intensity attacks as well.

For example, appeals to "sovereignty"[71] and "territorial sovereignty"[72] do not provide a firm legal basis for outlawing low-intensity cyber attacks. "Sovereignty" is difficult to apply in this context in part because some scholars and governments openly regard cyberspace as part of the global commons,[73] in which states cannot maintain or demand absolute control.[74] Additionally, there is no definitive understanding of how far a state's "territory" extends in cyberspace. Even if there were, the obligation to respect state sovereignty may merely be co-extensive with the prohibition on intervention, given that non-intervention is a direct corollary of state sovereignty.[75]

---

69. Draft Articles on State Responsibility, *supra* note 18, art. 2, at 68.

70. *See id.* arts. 30-31, 49.

71. *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 31 (2009); Schmitt, *supra* note 27; *see also* U.N. Charter art. 2, ¶ 1 (recognizing the "principle of the sovereign equality of all its Members").

72. *See, e.g.*, Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123 (2013), http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils [http://perma.cc/2LVQ-9Y8M]; *see also* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 35 (Apr. 9) ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations.").

73. *See, e.g.*, U.S. DEP'T OF DEF., STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005) ("The global commons consist of international waters and airspace, space, and cyberspace.").

74. *See* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 251-52 (8th ed. 2012).

75. Ian Brownlie explains that the "principal corollaries of the sovereignty and equality of states" include "(1) a jurisdiction, prima facie exclusive, over a territory and the permanent population living there; (2) a *duty of non-intervention* in the area of exclusive jurisdiction of other states." IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 289 (5th ed. 1998) (emphasis added); *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 128, ¶ 251 (June 27) ("The effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of non-intervention."); 1 OPPENHEIM'S INTERNATIONAL LAW, *su-*

Far more troublingly, historical practice weighs against any notion of an absolute right of sovereignty in cyberspace.[76] For centuries, states have remained passive about establishing a legal regime to deal with routine intrusions into state sovereignty, most notably intrusions in the form of covert action[77] and espionage.[78] Similarly, most states have been unwilling to accept a rigid ban on

pra note 59, at 428 (noting that non-intervention "is a corollary of every state's right to sovereignty, territorial integrity and political independence"); Kunig, *supra* note 59, ¶ 9 ("Without the prohibition of intervention, the principle of sovereignty could not be fully realized. Thereby, the raison d'être of the non-intervention rule is the protection of the sovereignty of the State.").

76. For more on why sovereignty and non-intervention should not be seen as absolute prohibitions for all activity falling below the threshold of the use of force, see Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 302 (2015) ("[I]deas such as non-intervention and sovereignty developed against a background understanding that states do and will spy on each other, thus establishing a carve-out for espionage within those very concepts.").

77. *See* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1074-75 (2006) ("There is little prospect . . . of concluding a convention defining the legal boundaries of intelligence gathering, if only because most states would be unwilling to commit themselves to any standards they might wish to impose on others."). *See generally* W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW (1992) (reviewing contemporary covert actions and intelligence policies).

78. *See* PHILLIP KNIGHTLEY, THE SECOND OLDEST PROFESSION: SPIES AND SPYING IN THE TWENTIETH CENTURY (1986); Yoo, *supra* note 27, at 190-91 (noting that espionage dates to ancient Greece, Rome, China, and Egypt). The prevalence of espionage—and more recently, cyber espionage—may remain a prime example of the *Lotus* principle at work: in the absence of international law to the contrary, states simply have the right to act freely. Armin von Bogdandy & Markus Rau, *The Lotus*, *in* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (June 2006), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e162 [http://perma.cc/F2SY-DPEL].

The U.S. government defines cyber espionage as "[o]perations and related programs or activities conducted . . . in or through cyberspace, for the primary purpose of collecting intelligence . . . from computers, information or communication systems, or networks with the intent to remain undetected." *Presidential Policy Directive—U.S. Cyber Operations Policy (PPD-20)* 2 (Oct. 2013), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf [http://perma.cc/X6TL-FSM3]. For the purposes of this Note, acts of cyber espionage are taken to be outside of the category of low-intensity cyber attacks to which liability applies, as they typically lack destruction or corruption of computer or internet systems and equipment. However, if an act of cyber espionage unintentionally or intentionally results in sufficient damage or coercion, it could then constitute a low-intensity cyber attack, or a traditional non-intervention, use of force, or armed attack under international law. *See* Yoo, *supra* note 27, at 183-84. The fact that the precise boundaries of the category of cyber espionage remain unsettled no doubt creates difficulties for defining the precise contours of any category of cyber attack. In addition, some cyber attacks may exhibit characteristics of both cyber espionage

all cross-border cyber infringements. In part, this is because a ban might limit their own cross-border covert intelligence, foreign political funding, and even cyber activities.[79] In addition, 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. At the same time, subsuming *all* low-intensity cyber attacks into the dark netherworlds of the legally unclear category of espionage would reflect a total inability of international law to prevent or even to provide redress for the resultant damages.

Given this apparent gap for low-intensity cyber attacks in international law, it appears less surprising that Secretary Kerry condemned North Korea for the Sony attack by vaguely stating that North Korea had "violated international norms," but without expressly referencing any violation of international law.[80] Similarly, President Obama simply called North Korea's attack "cyber vandalism," a term without any international legal meaning.[81] In this way, the State Department seemed to acknowledge the existence of such a gap, reflecting the State Department's focus on cyber attacks constituting a use of force.[82]

II. LIABILITY IN INTERNATIONAL LAW

In light of these challenges, this Part argues that there is not actually a severe *non liquet* in international law for cyber attacks that cause serious harm but fail to qualify as intervention and use of force. However, identifying state duties to address low-intensity cyber attacks requires turning away, at least initially, from the traditional concept of "wrongfulness" as affirmed in the *Draft Articles on State Responsibility* and toward the concept of "liability" in international law. This Part establishes the origin and nature of transboundary liabil-

and a low-intensity attack. However, for purposes of categorizing an attack (or part of an attack) as a low-intensity cyber attack, the attack must result directly in damage, as opposed to mere intrusion or extraction of information. In this context, it may be useful to note that many recent attacks on government entities, such as the Office of Personal Management, would not be categorized as low-intensity attacks as they have resulted mainly in information extraction.

79. *See* Chesterman, *supra* note 77, at 1075; Hathaway, *supra* note 35, at 49.

80. Press Release, John Kerry, *supra* note 10.

81. Eric Bradner, *Obama: North Korea's Hack Not War, But 'Cybervandalism*,' CNN (Dec. 24, 2014, 9:20 AM), http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism [http://perma.cc/TMZ6-W9WP].

82. *See* Koh, *supra* note 49, at 4.

ity, the duties and standards that it entails, and the relationship between a liability-based regime and the customary international law doctrine of state responsibility.

A. Liability and the Duty To Prevent and Redress Transboundary Harm

Historically, the duty to prevent and redress transboundary harm has roots in the Roman law maxim of *sic utere tuo ut alienum non laedas*, which states that each must use his property in a way that does not cause injury to another's.[83] This notion underlies the law of nuisance recognized in many legal systems around the world.[84] For example, English common law has long imposed a duty on property owners not to cause a nuisance that infringes upon another's use and enjoyment of his land.[85] French law similarly regards nuisance as the idea that "[n]o one may cause an abnormal degree of inconvenience in the neighborhood."[86]

At common law, *public* nuisance may be considered a criminal wrong and require a showing of infringement on property beyond that which is generally "suffered by the public."[87] In contrast, liability for *private* nuisance has long attached even where the defendant has used his land lawfully.[88] In these instances, liability results from a property owner's activities giving rise to "encroachment," "damage," or undue interference with a neighbor's "comfortable and

---

83. Elmer E. Smead, Sic Utere Tuo Ut Alienum Non Laedas*: A Basis of the State Police Power*, 21 CORNELL L.Q. 276, 276-77 (1936). Some scholars also point to the notion of *bon voisinage*, or "good neighborliness," as reflecting certain limitations (though not necessarily absolute) on states not to abuse the rights of other states. *See, e.g.*, Günther Handl, *Transboundary Impacts*, *in* OXFORD HANDBOOK OF INTERNATIONAL ENVIRONMENTAL LAW 533 (Daniel Bodansky et al. eds., 2008).

84. *See* 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, U.N. Doc. A/CN.4/543, *reprinted in* [2004] 2 Y.B. Int'l Law Comm'n pt. 1, at 85 [hereinafter ILC Survey].

85. *See id.* ¶ 56. Common law defines nuisance in tort as "an act or omission which is an interference with, disturbance of or annoyance to a person in the exercise or enjoyment of (a) a right belonging to him as a member of the public (public nuisance), or (b) his ownership or occupation of land or of some easement, profit or other right used or enjoyed in connection with land (private nuisance)." *Id.* ¶ 53 (quoting R.A. Buckley, *Nuisance*, *in* CLARK & LINDSELL ON TORTS 973 (18th ed. 2003)).

86. *Id.* ¶ 52 (translating the French, "*nul ne doit causer à autrui un trouble anormal du voisinage*").

87. *Id.* ¶ 53.

88. *Id.*

convenient enjoyment of his land."[89] In other words, "[i]t is sufficient in such cases for the victim to show the inconvenience and its abnormal character"; the plaintiff need not establish harm resulting from an act of negligence.[90]

In international law, the paramount case proclaiming liability for the duty to prevent and redress transboundary harm is the 1941 *Trail Smelter* arbitration between the United States and Canada. In assessing damages to the United States from sulfur dioxide pollution caused by a Canadian smelter, the tribunal held that "under the principles of international law . . . 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."[91]

Over the decades, the ICJ has also invoked the duty to prevent and redress transboundary harm on several occasions, mainly with respect to transboundary environmental damages. In its 1996 Advisory Opinion to the UN General Assembly on the legality of the threat of using nuclear weapons, the ICJ recognized "[t]he existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control," and noted that such an obligation is "now part of the corpus of international law relating to the environment."[92] The duty to prevent and redress transboundary harm has since played a role in a number of ICJ cases, including the court's 1997 *Gabčíkovo-Nagymaros Project* (*Hungary v. Slovakia*) judgment,[93] 2010 *Pulp Mills on the River Uruguay* (*Argentina v. Uruguay*) judgment,[94] and 2015 *Certain Activities Carried Out By Nicaragua in the Border Area* (*Costa Rica v. Nicaragua*) judgment.[95]

Several settlements for liability for the duty to prevent and redress transboundary harm have also taken place without much controversy. These include the 1957 *Lac Lanoux Arbitration* between France and Spain[96] and the Lake On-

89. *Id.*

90. *Id.* ¶ 52 (in French, "*un trouble anormal*"). The 1868 English case *Rylands v. Fletcher* noted that all significant harms, no matter "however innocently" inflicted, can give rise to liability in private nuisance. Rylands v. Fletcher [1868] 3 LRE & I. App. 330, 341 (HL) (Cranworth, J., concurring).

91. Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1965 (Trail Smelter Arb. Trib. 1941).

92. Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 241-42 (July 8).

93. Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 3, ¶ 53 (Sept. 25).

94. Pulp Mills on River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 18, ¶¶ 101, 193 (Apr. 20).

95. Certain Activities Carried Out by Nicaragua in Border Area (Costa Rica v. Nicar.), Judgment, 2015 I.C.J. 1, ¶¶ 177-217 (Dec. 16).

96. Lac Lanoux Arbitration (Fr. v. Spain), 12 R.I.A.A. 281 (1957).

tario Claims Tribunal established in 1965,[97] as well as dozens of arbitrations before ad hoc tribunals covering issues ranging from oil spills and factory pollution to damages caused by altering watercourses.[98]

While international tribunals have frequently addressed liability for transboundary harm in the environmental context,[99] there is no reason why liability cannot be applied to transboundary harms in other settings.[100] Indeed, history supports the application of liability for transboundary harm outside of the environmental context. Since the seventeenth century, scholars have recognized a duty to remedy cross-border harm in a variety of contexts. Grotius stated that from any "Fault or Trespass there arises an Obligation by the Law of Nature to make Reparation for the Damage, if any be done."[101] Even in his time, international law seemed to recognize a practice akin to liability: if one state owed tortious damages to another, the state's failure to remedy the harm could be a just cause of war itself.[102] For instance, states whose commercial vessels were dam-

97. Canada-United States Settlement of Gut Dam Claims, 8 I.L.M. 118, 133-42 (Lake Ontario Claims Trib. 1969).

98. *See* ILC Survey, *supra* note 84.

99. *See* World Summit on Sustainable Development, *Johannesburg Declaration on Sustainable Development*, U.N. Doc. A/CONF.199/20 (Sept. 4, 2002); U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. 1) (June 14, 1992) ("States have . . . the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."); U.N. Conference on the Human Environment, *Declaration*, U.N. Doc. A/CONF.48/14/Rev.1 (June 16, 1972) ("States have . . . the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."). The U.S. has recognized the principle of transboundary harm in the environmental context. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 601 (AM. LAW INST. 1987).

100. *See* GÖRAN LYSÉN, STATE RESPONSIBILITY AND INTERNATIONAL LIABILITY OF STATES FOR LAWFUL ACTS: A DISCUSSION OF PRINCIPLES 145-48 (1997) (describing debate on whether customary international law provides for liability outside of treaties and suggesting that it might). *But see* Allain Pellet, *The Definition of Responsibility in International Law*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 3, 10 (James Crawford et al. eds., 2010) (concluding that customary international law does not support a concept of liability outside of the environmental context).

101. HUGO GROTIUS, 2 THE RIGHTS OF WAR AND PEACE 884, ¶ 1 (Richard Tuck ed., Jean Barbeyrac trans., 2005) (1625); *see also* Pellet, *supra* note 100, at 5 (quoting Grotius and stating that his "formulation formed the very basis of international responsibility until very recently" and that it remains the foundation of the "classic theory" and "traditional definition").

102. *See* OONA HATHAWAY & SCOTT SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD 20-22 (forthcoming 2017) (unpublished manuscript) (on file with author).

aged by foreign ships could demand compensation not only from the owners of the ships but also from the flag states of the foreign ships as well. Remnants of this practice persist today. In 1971, Liberia accepted liability when the Liberian tanker *Juliana* ran aground off the coast of a Japanese island.[103] Likewise, in 1972, Canada cited *Trail Smelter* to remind the United States of its obligations when an oil tanker spilled near the state of Washington and polluted Canadian beaches.[104]

Over the course of the twentieth century, interest developed in clarifying how international law applies to the increasing number of harms made possible by the advancement of technology and growing interconnectedness of society.[105] In 1956, the International Law Commission (ILC) took up the project of codifying the law of state responsibility.[106] Though the project sought to define responsibility for wrongful international acts, there emerged an understanding that the "absence of wrongfulness [should] not prejudice compensation for damages caused by states to one another."[107] Based on this logic, the UN General Assembly invited the ILC in 1977 "to commence work on the topic of international liability for injurious consequences arising out of acts *not prohibited by international law*."[108] Since then, the ILC has produced dozens of reports on the topic of liability, including the 2001 *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*.[109] While the ILC project ultimately

---

103. *See* ILC Survey, *supra* note 84, ¶¶ 426-427.

104. *See id.*

105. *See* Michel Montjoie, *The Concept of Liability in the Absence of an Internationally Wrongful Act*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 100, at 503-04.

106. *See* James R. Crawford, *State Responsibility*, *in* MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. ¶ 6 (Sept. 2006), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093 [http://perma.cc/4TYZ-BTE3]; Robert Q. Quentin-Baxter (Special Rapporteur), *Fourth Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, ¶ 8, U.N. Doc. A/CN.4/373 (June 27, 1983) [hereinafter *Liability for Injurious Consequences*].

107. 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, 12 (1990).

108. Rep. of the Int'l Law Comm'n on the Work of Its Thirtieth Session, U.N. Doc. A/33/10, at 75 (1978) (emphasis added); *see also* ILC Survey, *supra* note 84, ¶¶ 1-4 (discussing the purpose of the survey as reviewing liability conventions for actions not prohibited by international law); Boyle, *supra* note 107, at 2-3 (noting that the ILC topic on "International Liability for the Injurious Consequences of Acts Not Prohibited by International Law" was an offshoot of the group charged with distilling the doctrine of state responsibility into the *Draft Articles on State Responsibility*).

109. Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities, with Commentaries, arts. 3, 7, 8, Rep. of the Int'l Law Comm'n on the Work of its Fifty-Third

dissolved, its conclusion with respect to liability remains relevant today:[110] where an activity "give[s] rise to loss or injury" across state boundaries, "reparation [is] due" unless the harm has long been tolerated "in accordance with the shared expectations of the States concerned."[111]

No doubt the capacity of humans to cause catastrophic harms beyond traditional state boundaries in an increasingly interconnected world heavily influenced the drafters of these ILC reports.[112] Yet while flood damage, pollution, mine explosions, and nuclear radiation are frequently discussed by the working group,[113] ILC Special Rapporteur Robert Quentin-Baxter noted that there was "never an intention to propose a reduction in the scope of the topic to questions of an ecological nature, or to any other subcategory of activities involving the physical uses of territory."[114]

Session, U.N. Doc. A/56/10, at 370-77 (2001) [hereinafter Draft Articles on Transboundary Harm]; *see, e.g.*, G.A. Res. 65/28 (Dec. 6, 2010); G.A. Res. 62/68 (Dec. 6, 2007).

110. As James Crawford has recalled, "Despite the uncertainty surrounding their future status, the Draft Articles [on Transboundary Harm] provide an authoritative statement of the scope of a state's international legal obligation to prevent a risk of transboundary harm." CRAWFORD, *supra* note 74, at 357.

111. *Liability for Injurious Consequences*, *supra* note 106, annex § 4. Perhaps the most enduring aspect of the ILC's work is its affirmation of the underlying *purpose* of liability. In the words of the ILC Rapporteur, Quentin-Baxter, "[I]f all transboundary harm were wrongful, there would be no need for this topic. Every activity that caused or threatened such harm would be prohibited, except with the consent of the States whose interest was affected." Robert Q. Quentin-Baxter (Special Rapporteur), *Second Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, ¶ 85, U.N. Doc. A/CN.4/346 (July 1, 1981).

112. *See Liability for Injurious Consequences*, *supra* note 106, ¶ 60 (noting that as "international life grows more complex and is more elaborately organized," liability, as opposed to wrongfulness, will be a more appropriate form of accountability); *see also* 4 MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 214 (Rudolf Bernhardt ed., 2000) ("[S]cientific and technological advances . . . have obliged international law to adapt itself to new circumstances . . . . The problem posed by these new activities does not derive from the question whether they are legitimate or wrongful, but from the fact that, even if they are essential or beneficial, they embody an inherent risk of transboundary harm.").

113. *See* ILC Survey, *supra* note 84. *See generally Analytical Guide to the Work of the International Law Commission*, INT'L L. COMMISSION, http://legal.un.org/ilc/guide/gfra.shtml [http://perma.cc/SB6V-6GSK] (organizing the work of the ILC by topics and helpfully tracking the development of each topic).

114. *Liability for Injurious Consequences*, *supra* note 106, ¶ 17 ("[T]here is a rather general expectation that the field of application will include all physical uses of territory giving rise to adverse physical transboundary effects."). Initially, the ILC project of codifying liability was conceptualized in rather broad terms. *See* Boyle, *supra* note 107, at 96. For example, a 1995 ILC survey suggested that liability might extend to airspace, nuclear or industrial activities, conservation and utilization of critical resources, and even communication and broadcasting.

Outside of the ILC process, several prominent cases have appeared to apply transboundary liability in non-environmental contexts. In the 1948 *Corfu Channel* case, the Permanent Court of International Justice (PCIJ) held Albania responsible to the United Kingdom for mines laid in violation of "[e]very State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[115] When read closely, it appears that the court

See Liability Regimes Relevant to the Topic "International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law": Survey Prepared by the Secretariat, [1995] 2 Y.B. Int'l Law Comm'n pt. 1, at 61, U.N. Doc. A/CN.4/471. Documents suggest that a debate existed between those who rejected the idea of focusing on the environment and those who believed that liability should also cover transboundary harm from activities as disparate as antitrust laws, monetary policies, newspapers, and even medical and biological research. *See* Daniel Barstow Magraw, *Transboundary Harm: The International Law Commission's Study of "International Liability"*, 80 AM. J. INT'L L. 305, 323-24 (1986) ("Some members argued—without providing any substantial justification—for the inclusion of 'restrictive economic policies,' 'monetary activities' and 'transboundary economic problems' (possibly involving such subjects as antitrust policies, restrictive tariffs and import quotas, inflationary and deflationary monetary policies, international lending policies, and tax laws affecting transfer pricing or transnational capital flows). Others asserted that medical and biological research and, more generally, 'economic, industrial and other activities' should be included. Those and other claims prompted counter-arguments against coverage of transboundary harm caused by newspaper articles, monetary devaluation and legitimate industrial or agricultural competition.").

In the end, the ILC working group compromised: the decision was made that the "rules to be drawn up should be of a general nature," even though many would relate to the environment. *See* M.B. Akehurst, *International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, 16 NETH. Y.B. INT'L L. 3, 4 (1985) (noting that while Quentin-Baxter himself preferred to limit the topic to the "field of the environment," the ILC as a whole explicitly rejected this approach).

This ILC project has been subject to sharp criticism. Brownlie calls the Commission "fundamentally misconceived." IAN BROWNLIE, SYSTEM OF THE LAW OF NATIONS: STATE RESPONSIBILITY PART I 50 (1983); *see also* JULIO BARBOZA, THE ENVIRONMENT, RISK AND LIABILITY IN INTERNATIONAL LAW 125 (2011) (explaining a serious attack made on the ILC's work in 1997 resulting from confusion that Barboza believes could have been, and in part was, ultimately overcome). Most take a more moderate approach, recognizing that despite the problems encountered by the ILC in its efforts to develop a general regime of liability, the utility and purpose of such a system is nontrivial. *See, e.g.*, Mahnoush H. Arsanjani & W. Michael Reisman, *The Quest for an International Liability Regime for the Protection of the Global Commons*, *in* INTERNATIONAL LAW: THEORY AND PRACTICE 469, 488 (Karl Wellens ed., 1998) ("Our review of the successive efforts to deal with harm to the global commons thus indicates a quest for an effective legal regime that has, as yet, had very limited success. . . . The problems in constructing a viable regime for the protection of the global commons that incorporates a liability component are . . . formidable. But the consequences of not fashioning such a regime—and doing it soon—may well constitute the most profound common threat to humanity in the twenty-first century."); Montjoie, *supra* note 105, at 504.

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

recognized the novelty of transboundary liability, particularly liability for military-like actions *outside of the context of war*, but applied it nonetheless—even to non-environmental damages. As it explained, the duty not to cause harm to another state is expansive in contemporary society; in fact, it is a duty "*even more exacting* in peace than in war."[116] Scholars have suggested that *Corfu Channel* recognized a "basic" transboundary duty upon states in international law "not . . . to act as to injure the rights of other states."[117] Indeed, building on *Corfu Channel*, several states have successfully sought compensation for transboundary harm from weapons tests.[118]

B. Liability and the Articles on State Responsibility

In light of this international practice, why is an act of transboundary harm not "wrongful," and how is liability different from state responsibility? This Section explains that when transboundary harm occurs as the result of an otherwise lawful activity, a state may become liable to compensate the injured party for any harm caused. At that point, the state has not yet violated an obligation of international law; however, if the state fails to pay reparations, it becomes responsible for violating the duty to prevent and redress transboundary harm.

---

116. *Id.* (emphasis added).

117. MALCOLM N. SHAW, INTERNATIONAL LAW 851 (6th ed. 2008). Shaw notes that the U.S. Attorney General expressed support for this doctrine in 1895. *Id.* at 851 n.28.

118. For example, in 1955, the United States agreed to pay Japan for damages caused to individuals, fish populations, and the Japanese fish market due to nuclear tests carried out by the United States on Enewetak Atoll. In 1964, the United States authorized $950,000 to be paid in compensation to the inhabitants of Rongelap Atoll for similar damages, while in later decades it prepared to settle Marshall Islands claims totaling over $100 million. Elsewhere, Canada reserved its right to compensation in the event of damage to the Pacific resulting from nuclear tests on Amchitka Island in 1960, while Japan and New Zealand made a variety of tort demands with respect to French nuclear testing throughout the decades. Similarly, several European states reserved the right to bring claims against the Soviet Union for damages caused by Chernobyl. *See* ILC Survey, *supra* note 84, ¶¶ 404-412.

Two other examples illustrate the duty to prevent and redress transboundary harm outside of the environmental context. In 1949, Austria made a formal protest to the Hungarian Government not to install land mines near the Austrian border. When mines detonated in Austria nearly two decades later, the Austrian government condemned Hungary's actions, relying explicitly on the principle of "good-neighbourliness." *Id.* ¶ 419. Similarly, in 1968, the Swiss government recognized liability to compensate Liechtenstein for damages suffered when a Swiss artillery unit erroneously fired shells across the border. *See id.* ¶ 420.

First, we must distinguish between primary and secondary duties (also referred to as "rules" or "obligations") in international law.[119] Primary duties govern state conduct. An example of a primary duty is the prohibition against intervention. Secondary duties impose remedial obligations on states for acts that violate a primary duty and are attributable to the state, taking into account pertinent circumstances and defenses (such as duress and necessity).[120] An example of a secondary duty is the requirement to make reparations. Primary duties typically arise from treaties, customary international law, or general principles of international law, while secondary duties are often found in the *Draft Articles on State Responsibility*.[121] Therefore, to understand when a state has committed a "wrongful act," one must first turn to the primary duty in question and determine whether it has been breached.

---

119. *See* Eric David, *Primary and Secondary Rules*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 100, at 27.

120. *See* Draft Articles on State Responsibility, *supra* note 18, arts. 20-27, at 173-211. For further discussion on primary and secondary duties, see Boyle, *supra* note 107, at 10-11. The Commentary to the *Draft Articles on State Responsibility* suggests that secondary duties concern the following issues:

> (a) The role of international law as distinct from the internal law of the State concerned in characterizing conduct as unlawful; (b) Determining in what circumstances conduct is to be attributed to the State as a subject of international law; (c) Specifying when and for what period of time there is or has been a breach of an international obligation by a State; (d) Determining in what circumstances a State may be responsible for the conduct of another State . . . ; (e) Defining the circumstances in which the wrongfulness of conduct under international law may be precluded; (f) Specifying the content of State responsibility, i.e. the new legal relations that arise from the commission by a State of an internationally wrongful act, in terms of cessation of the wrongful act, and reparation for any injury done; (g) Determining any procedural or substantive preconditions for one State to invoke the responsibility of another State, and the circumstances in which the right to invoke responsibility may be lost; (h) Laying down the conditions under which a State may be entitled to respond to a breach of an international obligation by taking countermeasures designed to ensure the fulfilment of the obligations of the responsible State under these articles.

Draft Articles on State Responsibility, *supra* note 18, at 60.

121. *See* Boyle, *supra* note 107, at 10; Draft Articles on State Responsibility, *supra* note 18, at 123; James Crawford (Special Rapporteur), *Third Rep. on State Responsibility*, ¶ 325, U.N. Doc. A/CN.4/507/Add.3 (Aug. 4, 2000) ("The law of treaties is concerned essentially with the content of primary rules and with the validity of attempts to alter them; the law of responsibility takes as given the existence of the primary rules . . . and is concerned with the question whether conduct inconsistent with those rules can be excused and, if not, what the consequences of such conduct are.").

Liability differs from the traditional concept of responsibility. According to the *Draft Articles on State Responsibility*—the primary restatement of the doctrine of state responsibility, prepared by the ILC—a state is responsible for an act (or omission) when the act is attributable to the state and wrongful under international law. An act is wrongful under international law when it is a violation of a state's primary duty to another state.[122] In contrast, liability does not result from a wrongful act per se[123] but instead focuses on compensation for harms.[124] Under this second approach, a state can be liable for an act of transboundary harm, even if the activities giving rise to the harm were not in themselves breaches of international law.[125]

Within this two-tiered system of state responsibility, the duty to prevent and redress transboundary harm is unusual, because it appears to contain aspects of both a primary and a secondary duty. As a primary duty, it incorpo-

122. SHAW, *supra* note 117, at 782.

123. An American member present at the ILC's 25th Session is said to have initially made the distinction between the terms "liability" and "responsibility." The record reflects that he advocated: "[T]he term 'responsibility' should be used only in connexion [sic] with internationally wrongful acts and that, with reference to the possible injurious consequences arising out of the performance of certain lawful activities, the . . . term 'liability' should be used." *Draft Rep. of the Commission on the Work of Its Twenty-Fifth Session*, [1973] 1 Y.B. Int'l Law Comm'n 210, 211, U.N. Doc. A/CN.4/SER.A/1973.

124. The ILC has stressed the importance of harm to liability, as opposed to responsibility. *See State Responsibility*, [1974] 1 Y.B. Int'l Law Comm'n 5, 7, U.N. Doc. A/CN.4/SER.A/1974 ("In the case of wrongful activities, damage was often an important element, but it was not absolutely necessary as a basis for international responsibility. On the other hand, damage was an indispensable element for establishing liability for lawful, but injurious activities."). A number of commentators, including the ILC, refer to liability for transboundary harm as thus liability *sine delicto*, that is, liability "which does not have its origin in an internationally wrongful act." *See* RENÉ LEFEBER, TRANSBOUNDARY ENVIRONMENTAL INTERFERENCE AND THE ORIGIN OF STATE LIABILITY 15, 198-202 (1996).

125. Several of the handful who have examined the topic of liability in international law begin by noting how much "confusion" there is about the subject. *See, e.g.*, Alan Boyle, *Liability for Injurious Consequences of Acts Not Prohibited by International Law*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 100, 95, 95-104 (noting the confusion surrounding how the ILC working group on injurious consequences would develop the topic and the variety of intellectual difficulties that the ILC faced); N.L.J.T. Horbach, *The Confusion About State Responsibility and International Liability*, 4 LEIDEN J. INT'L L. 47 (1991) (recognizing the confusion between state responsibility and international liability); Sompong Sucharitkul, *State Responsibility and International Liability Under International Law*, 18 LOY. L.A. INT'L & COMP. L.J. 821 (1996) (same); *see also Rep. of the International Law Commission on the Work of Its Thirty-Seventh Session*, U.N. Doc. A/40/10, *reprinted in* [1985] 2 Y.B. Int'l Law Comm'n pt. 2, at 19-27 (discussing the various intellectual challenges and disagreements encountered by the ILC in its work on liability). There is still confusion left about the state of liability in international law.

rates the standards of care expected of states to fulfill the duty.[126] Yet like a secondary duty, it requires states to provide remedies when harms occur.[127] This combination of duties comprises "liability" in international law.[128] Liability is thus a "continuum of prevention and reparation" resulting from the underlying duty to prevent and redress transboundary harm.[129]

These distinctions have caused much confusion over the years, as scholars have debated whether transboundary harms automatically give rise to state responsibility instead of liability. As ICJ Judge Higgins explains, "Cases like *Trail Smelter*—which we had all in our youth thought [had] something to do with international responsibility for harm to your neighbour (and a clear example of the absence of need of malice, or *culpa*)," are instead "*not* now questions of state responsibility but are put into another category"—what today is called international liability.[130]

Though distinct from responsibility, liability remains connected to responsibility in an important way. While causing transboundary harm is not prohibited by international law, "responsibility attach[es] for harm, [when] coupled with a [state's] failure to meet the required standard of care."[131] As Judge Higgins explains, "[F]ailure to meet [the applicable] standard of care, with result-

---

126. The ILC conceives of prevention as: (1) performing proper risk assessments, (2) preventing harm or minimizing the risk thereof, and (3) giving notice and technical information concerning risk to the country affected. *See* Draft Articles on Transboundary Harm, *supra* note 109, at 390, 402, 406.

127. *See* Boyle, *supra* note 107, at 10, 17. Boyle notes that within the international liability regime, the ILC has recognized that an "injured State can order the other to: (1) discontinue the act; (2) apply national legal remedies; (3) re-establish the situation existing before the act or, to the extent that this is impossible, pay corresponding compensation; (4) provide guarantees against repetition." *Id.* at 17. However, some have disagreed, suggesting that *only compensation* can be requested. *See id.* at 17-18; *see also* Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, Advisory Opinion, Case No. 17, Order of Feb. 1, 2011, ITLOS Rep. 10, 49 (advising, with regard to international seabed activity, that sponsoring States are required to "establish procedures, and, if necessary, substantive rules governing claims for damages before its domestic courts").

128. Outside of customary international law and general principles of international law, several treaties have created forms of liability in international law. *See infra* text accompanying note 143.

129. *Liability for Injurious Consequences*, *supra* note 106, ¶ 40. Others have called this same underlying duty a "compound primary obligation." Magraw, *supra* note 114, at 311.

130. *See, e.g.*, ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 164 (1995).

131. *Id.* at 165.

ant harm—*that* is the internationally wrongful act, for which state responsibility attaches."[132]

Cases like *Trail Smelter* and *Corfu Channel* can be seen as imposing state responsibility *after* the state that caused transboundary harm failed to redress the situation. These cases typically involve states that failed to terminate and compensate for activities resulting in cross-border harm even after having received notice. Moreover, these cases involve transboundary harms resulting from activities that are not themselves unlawful under international law. Therefore, although some see *Trail Smelter* and *Corfu Channel* as establishing the idea that transboundary harm is wrongful under international law,[133] these cases are better understood as invoking the concept of wrongfulness for transboundary harm only after the initial harms are inadequately redressed.

Under customary international law, states have long refrained from judging certain kinds of cross-border damages as wrongful in and of themselves—provided that the state causing the damage takes remedial action to compensate for the damage.[134] Under this liability regime, the state causing the transboundary harm must fail to provide redress before the injured state can invoke state responsibility. Until this point, the transboundary harm is not yet a "wrongful act" and the injured state cannot engage in countermeasures. This conception of liability helps prevent routine cross-border harms, especially unintentional harms, from escalating within the international legal system.

C. Dual Liability Standards

Even once we recognize that international law can impose liability for transboundary harms, we must decide what standard of care should be used to determine whether a state is liable. The *Draft Articles on State Responsibility* deliberately do not provide guidance as to the appropriate standard of care in any particular context.[135] Instead, the *Draft Articles on State Responsibility* defer to

---

132. *Id.*

133. *Id.*

134. *Id.* at 163-64. As Oona Hathaway and Scott Shapiro explain, in the pre-contemporary order, this practice played out clearly not via the *Draft Articles on State Responsibility*, which prohibit a recourse to force as a means of secondary enforcement in the contemporary era, but indeed via the secondary enforcement tool of war: "[States] had to make a claim regarding a wrong, offer an opportunity for peaceful redress, explain to the world why the wrong had not [been] addressed, and *then* go to war." *See* HATHAWAY & SHAPIRO, *supra* note 102, at 9.

135. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 13-14 (2002) ("[T]he essential point is surely this, that different primary rules of international law impose different standards rang-

primary rules to determine whether "some degree of fault, culpability, negligence or want of due diligence" applies in assessing state conduct.[136] This is a sensible approach because, as Judge Higgins suggests,

> [t]he standard by which the duty of care in regard to an obligation is to be tested is determined *by reference to the particular requirements of that obligation*. The law of state responsibility does not tell us the answer to this: we can say only that a state is responsible for failing to take, either generally or with respect to the conduct of individuals, duly diligent care or care to such other standard as the particular obligation requires.[137]

While some suggest that the *Draft Articles on State Responsibility* impose negligence as a default standard of care when the primary rule is unclear about

---

ing from "due diligence" to strict liability . . . . By referring these issues to the interpretation and application of the primary rule, the Draft Articles took an essentially neutral position, neither requiring nor excluding these elements in any given case. This was a more subtle approach, more appropriate to a general set of articles dealing with all international obligations . . . .").

136. *Id.* at 82. Some argue that in the case of *Bosnia & Herzegovina v. Serbia & Montenegro*, the ICJ settled the question of what the proper standard of liability was when it stated the following: "A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide." Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 430 (Feb. 26). However, in that case, it is clear that the ICJ did not set out a universal standard of due diligence, but instead looked to "the obligation in question" (the relevant primary duty, which was a duty to prevent genocide). In doing so, the ICJ determined that the duty to prevent genocide was "one of conduct and not one of result," and thus that a standard of due diligence was applicable. *Id*.

137. HIGGINS, *supra* note 130, at 157; *see also* Draft Articles on State Responsibility, *supra* note 18, at 31 ("The emphasis is on the secondary rules of State responsibility; that is to say, the general conditions under international law for the State to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom. The articles do not attempt to define the content of the international obligations, the breach of which gives rise to responsibility. This is the function of the primary rules, whose codification would involve restating most of substantive customary and conventional international law."); R. DOAK BISHOP, JAMES E. CRAWFORD & W. MICHAEL REISMAN, FOREIGN INVESTMENT DISPUTES: CASES, MATERIALS, AND COMMENTARY 576 (2d ed. 2014) ("Although international responsibility is sometimes said to be based on the principle of 'objective responsibility,' there is no general rule in the matter: some obligations are obligations of due diligence, others may entail a stricter standard.").

the applicable standard of care,[138] many primary duties require stricter or more lenient standards of care.[139]

The ILC suggests that the duty to prevent and redress transboundary harm is one such primary duty—in certain circumstances, it may impose strict or absolute liability. Strict liability is liability without fault, meaning that liability is imposed on the actor regardless of whether reasonable care was exercised.[140] While similar, absolute liability imposes liability regardless of the actor's potential defenses or intent.[141]

As Justice Blackburn explained in *Rylands v. Fletcher*, industrial society has recognized the need for strict liability for "anything *likely* to do mischief if it escapes" and "which [the owner] *knows* will be mischievous if it gets on to his neighbor's [property]."[142] Based on this reasoning, domestic jurisdictions throughout the world, as well as international treaties, recognize liability without "fault" for "abnormally dangerous" or "ultra-hazardous" activities, often in the areas of nuclear energy, transportation of hazardous chemicals, environmental damage, pollution, oil spills, train wrecks, space objects, and mining.[143]

Some have even suggested that absolute liability might apply beyond this practice to inherently hazardous activities. For example, Canada referenced absolute liability as a "general principle" of international law in its claim against the Soviet Union for damages caused by the "Cosmos 954" satellite.[144] Similar-

---

138. *See* Sucharitkul, *supra* note 125, at 835-39. Nevertheless, Malcolm Shaw has contended that the majority of academic opinions tend toward an understanding of strict liability and the objective theory for state responsibility. *See* MALCOLM SHAW, INTERNATIONAL LAW 698 (5th ed. 2003).

139. *See, e.g.*, Convention on the International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2398, 961 U.N.T.S 187; Vienna Convention on Civil Liability for Nuclear Damage, May 21, 1963, 1063 U.N.T.S. 265; Convention on Third Party Liability in the Field of Nuclear Energy, July 29, 1960, 956 U.N.T.S. 263.

140. *See* JAMES A. HENDERSON, JR. ET AL., THE TORTS PROCESS 451 (8th ed. 2012).

141. *See id.* Absolute liability is taken to mean full liability, or in the words of Judge Higgins, liability "by reference to events, with *culpa* as much an irrelevance as the due-diligence test." HIGGINS, *supra* note 130, at 161. Absolute liability is used over the term "strict liability" to avoid confusion from the fact that the strict liability is typically only referenced in the context of negligence torts.

142. Rylands v. Fletcher [1868] LRE & I. App. 330, 339-40 (HL).

143. ILC Survey, *supra* note 84, ¶ 21; *see, e.g.*, United Nations Convention on the Law of the Non-Navigational Uses of International Watercourses, May 21, 1997, 36 I.L.M. 700; United Nations Convention on Civil Liability for Damage Caused During Carriage of Dangerous Goods by Road, Rail and Inland Navigation Vessels, Oct. 10, 1989, U.N. Doc. ECE/TRANS/79; *see also supra* note 139 (listing additional treaties).

144. ILC Survey, *supra* note 84, ¶ 401.

ly, the ILC has suggested that in some areas, states have been held liable for harms even when they took care to prevent them.[145] Malcolm Shaw explains that the key benefit of the absolute liability approach is that it "mov[es] the burden of proof and shift[s] the loss clearly from the victim to the state," as a plaintiff need not show that a state causing harm actually acted imprudently but only that harms emanated from its activities or territory.[146]

Nevertheless, the ILC acknowledges that most domestic legal systems have increasingly imported the concept of negligence into nuisance doctrine, and therefore that the duty to prevent transboundary harm is better seen as imposing a negligence standard.[147] Negligence is defined as failure to behave with the level of care that a reasonable person would have exercised under the circumstances.[148] The concept of negligence finds its way into international liability in the form of the standard of due diligence, which requires states to act with care that "is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance."[149] In the *Pulp Mills* case, the ICJ referred to the PCIJ's judgment in *Corfu Channel*[150] and recognized "an obligation [on states] to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party."[151] The court further explained due diligence as

> 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 pri-

---

145. The ILC has at points noted that even if the acting state observes its duties to take preventive measures, it should nonetheless be held answerable for damage, given that the duty not to cause damage is un-conditional. *See* XUE, *supra* note 24, at 14.

146. SHAW, *supra* note 117, at 888.

147. *See* ILC Survey, *supra* note 84, ¶¶ 65-79.

148. *See* HENDERSON ET AL., *supra* note 140, at 159.

149. SHAW, *supra* note 117, at 861. *See generally* ILA Study Grp. on Due Diligence in Int'l Law, *First Report*, INT'L L. ASS'N (Mar. 7, 2014), http://www.ila-hq.org/download.cfm/docid/8AC4DFA1-4AB6-4687-A265FF9C0137A699 [http://perma.cc/786K-TDCU] (considering whether there is agreement between the distinctive areas of international law in which the concept of due diligence is applied). Due diligence was first recognized in the *Alabama* arbitration of 1872 between the United States and the United Kingdom over obligations under the law of neutrality. *See* Ala. Claims Arbitration, (U.S. v. Gr. Brit.), 29 R.I.A.A. 125, 129 (1872). Due diligence also evolved out of the customary international duty on states to protect aliens. *See* ILA Study Grp. on Due Diligence in Int'l Law, *supra*, at 2.

150. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 24 (Apr. 9).

151. Pulp Mills on River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 18, ¶ 197 (Apr. 20).

vate operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party.[152]

Yet it remains unclear which of these two standards is most appropriate for the duty to prevent transboundary harm. Negligence has been found alternatingly essential and irrelevant to liability for transboundary harm in different cases.[153] There is also extensive disagreement over how to interpret the few cases that have dealt explicitly with transboundary liability. For instance, some observe that because the United States did not "affirmatively prove the defendant's negligence or wilful default" in *Trail Smelter*, strict liability effectively applied.[154] Others make a similar argument with respect to the Lake Ontario Claims Tribunal, arguing that the Tribunal made no express finding of fault or negligence for the damages that resulted from extensive flooding in connection with a Canadian-built dam.[155]

Disagreement also persists over the standard applied by the ICJ in *Corfu Channel*. The most persuasive views, supported by the dissents of Judges Badawi Pasha and Winiarski, suggest that *Corfu Channel* stands for strict liability in certain situations, given that the breach of the duty to prevent transboundary harm was recognized without proof of negligence.[156] The dissenting judges argued that Albania had neither breached any duty of diligence nor acted with willful default, and instead that the court had applied a higher standard, what they called "absolute" liability.[157]

A way out of this dissensus can be found in *Nuclear Tests (Australia v. France)*.[158] In the ICJ hearings in the case, Australia argued that there is a

---

152. *Id*. For instance, in the environmental context, due diligence has since become firmly established as a requirement on states to undertake environmental impact assessments prior to activities likely to give rise to significant harm, as well to notify and consult parties likely to be affected by that harm and offer technical assistance in the case that harm does occur. *See, e.g.*, Draft Articles on Transboundary Harm, *supra* note 109, art. 8, at 406-09 (specifying that states should notify and consult other states if there is a risk that one of their activities may cause harm and also obliging states to provide reparation, consequential on the causation of harm itself); Boyle, *supra* note 107, at 22.

153. The ILC has noted as much in its survey of state practice on liability. *See* ILC Survey, *supra* note 84, ¶ 55.

154. *Id.* ¶ 229.

155. *See id.* ¶¶ 415-16.

156. *See id.* ¶¶ 228-29.

157. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 51 (Apr. 9) (Winiarski, J., dissenting); *id.* at 66-67 (Badawi Pasha, J., dissenting); ILC Survey, *supra* note 84, ¶ 229.

158. Nuclear Tests (Austl. v. Fr.), Order, 1973 I.C.J. 99 (June 22). The ICJ did not rule on the merits of this case.

growing trend toward a due diligence standard for activities holding societal value,[159] but strict liability for those imposing unreasonable risks without clear benefits. While "every transmission by natural causes of chemical or other matter from one State into another State's territory, air space or territorial sea automatically created a legal cause of action in international law without the need to establish anything more," contemporary state practice has in fact "modified the application of this principle in respect of the interdependence of territories."[160] Therefore, in Australia's view, liability standards should be more lenient when the activities causing harm "are generally regarded as natural uses of territory in a contemporary society and . . . while perhaps producing some inconvenience, they have a community benefit."[161] The ICJ seemed to adopt this approach in *Nuclear Tests* when it found France's activities to have "no compensating benefit to justify New Zealand's exposure to such harm."[162]

Therefore, we can reconcile these competing standards by recognizing that while private nuisance has long looked favorably upon absolute liability for

---

159. Article 10 of the ILC's *Draft Articles on Transboundary Harm* similarly supports an "equitable balance of interests" based in part upon "importance of the activity, taking into account its overall advantages of a social, economic and technical character . . . in relation to the potential harm" when consulting potentially harmed states about preventative measures. Draft Articles on Transboundary Harm, *supra* note 109, art. 10, at 412. Boyle notes that one of the three main points driving the work of the ILC on liability was thus the idea that "every State must have the maximum freedom of action within its territory compatible with respect for the sovereign equality of other States." Boyle, *supra* note 107, at 6.

160. ILC Survey, *supra* note 84, ¶ 234; *see also Nuclear Tests*, 1973 I.C.J. at 104.

161. ILC Survey, *supra* note 84, ¶ 234; *see also* SHAW, *supra* note 117, at 861 (noting that the ILC *Draft Articles on Transboundary Harm* specify in Article 10 that the Articles strive for an "equitable balance of interests" and that in applying liability, the *Draft Articles on Transboundary Harm* seek to account for the "the importance of the activity [causing harm]" for the state where the activity is taking place in relation to the states that are likely to be affected, as well as the "means of preventing or minimising such risk").

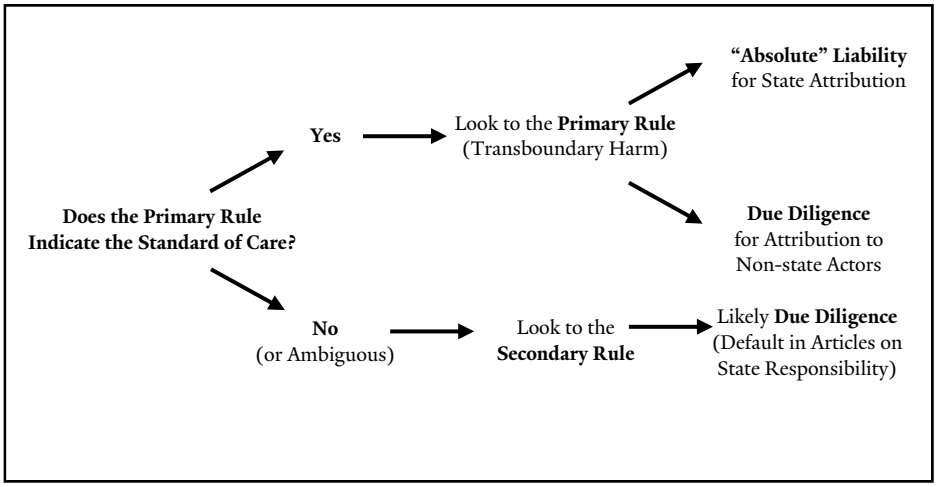
162. ILC Survey, *supra* note 84, ¶¶ 235-37. The ILC has made similar references to the fact that some activities giving rise to transboundary harm are "not always possible to prohibit or avoid" because they are "beneficial to society in general." Pemmaraju Sreenivasa Rao (Special Rapporteur), *Third Rep. on the Legal Regime for the Allocation of Loss in Case of Transboundary Harm Arising Out of Hazardous Activities*, ¶ 36(3), U.N. Doc. A/CN.4/540 (May 15, 2004). Because of this, the ILC has noted that in many jurisdictions,

> Strict liability . . . [for] inherently dangerous or hazardous activities . . . is arguably a general principle of international law, or in any case could be considered as a measure of progressive development of international law. In the case of activities which are not dangerous but still carry the risk of causing significant harm, there is perhaps a better case for liability to be linked to fault or negligence.

Id. ¶ 38.

otherwise "abnormal" activities that do not benefit the community, due diligence has been more accepted for activities that cause harm but are thought to promote a common good. A dual approach of this sort recognizes that not all transboundary harms exist in the same light, particularly if imposing absolute liability would result in onerous burdens or infringements on other important principles, such as privacy and open internet access. This approach is particularly apt for the cyber context, as discussed next.

FIGURE 2.
STANDARDS OF LIABILITY AND RESPONSIBILITY UNDER INTERNATIONAL LAW



III. APPLYING LIABILITY FOR TRANSBOUNDARY HARM TO LOW-INTENSITY STATE-SPONSORED CYBER ATTACKS

> "[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."
>
> –Mark Stroh, National Security Council Spokesman[163]

This Part applies the concept of liability to low-intensity state-sponsored cyber attacks and discusses how the appropriate standard of care should depend on whether a cyber attack is attributable to a state or non-state actor.

A. Contemporary Approaches and Cyber: An Absurd Result?[164]

Recent scholarship has begun to import features of the duty to prevent transboundary harm into the cyber context.[165] Most notably, this concept surfaces in the *Tallinn Manual*.[166] Some have suggested that states have a "due dil-

---

163. Julie Makinen, *North Korea Decries U.S. Allegations on Sony Hack; U.S. Turns to China*, L.A. TIMES (Dec. 20, 2014), http://www.latimes.com/world/asia/la-fg-north-korea-proposes-joint-investigation-into-sony-hack-20141220-story.html [http://perma.cc/8VPD-J5CT].

164. This is a term adopted from treaty interpretation. *See* Vienna Convention on the Law of Treaties art. 32, May 23, 1969, 1155 U.N.T.S. 331 ("Recourse may be had to supplementary means of interpretation . . . when the interpretation according to article 31 . . . [l]eads to a result which is manifestly absurd or unreasonable.").

165. *See* Oren Gross, *Cyber Responsibility To Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481 (2015); Jason Healey & Hannah Pitts, *Applying International Environmental Legal Norms to Cyber Statecraft*, 8 I/S 356 (2012); Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 275 (2015); Thilo Marauhn, *Customary Rules of International Environmental Law—Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 46; Daniel Ortner, *Cybercrime and Punishment: The Russian Mafia and Russian Responsibility To Exercise Due Diligence To Prevent Trans-boundary Cybercrime*, 2015 BYU L. REV. 177; Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68 (2015); Ziolkowski, *supra* note 46; Jan E. Messerschmidt, Note, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275 (2013).

166. *See* TALLINN MANUAL, *supra* note 48, r. 5, at 26 ("A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states."); *see also* U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/172 (July 22, 2015) (transmitting member states' views of international security in the cyber context); Group of Governmental Experts in the Field of Infor-

igence obligation with respect to both government and private cyber infrastructure on, and cyber activities emanating from, their territory."[167] In this framing, a state that fails to meet this due diligence standard of care is held responsible under international law and may be subject to countermeasures.[168]

Beginning with the issue of transboundary harm, the *Tallinn Manual* suggests that due diligence is either itself a primary obligation in international law, or else a standard of care owed with respect to the principle of territorial sovereignty.[169] Michael Schmitt is equally vague; for him, due diligence is a "principle" of international law on its own but at the same time, one that "derives from the principle of sovereignty."[170]

To consider due diligence to be a primary obligation is problematic. Due diligence appears to exist not as an independent obligation within customary international law, giving rise to state responsibility, but instead as a standard of care owed *with respect to* certain primary duties in international law.[171] But the second option—deriving a due diligence standard from the principle of sovereignty—may also present challenges, particularly in the cyber context. For one, as Part I discussed, considerable issues arise in attempting to apply the notion of sovereignty to cyberspace. Not only is it difficult to determine the extent of a state's sovereign territorial rights in the internet, but there are also significant arguments against an absolute right of states to sovereignty in the first place. Moreover, critics point to hundreds of years of state practice suggesting that

mation and Telecommunications in the Context of Information Security, ¶ 23, U.N. Doc. A/68/98 (June 24, 2013) ("States should seek to ensure that their territories are not used by non-State actors for unlawful use of [information and computer technologies].").

167. Schmitt, *supra* note 165, at 70.

168. *See id.* at 70; Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent*, 201 MIL. L. REV. 1, 14 (2009).

169. *See* TALLINN MANUAL, *supra* note 48, r. 5, at 26-29.

170. *See* Schmitt, *supra* note 165, at 71.

171. For instance, in the *Alabama* arbitration, the foundational case affirming the concept of due diligence in international law, the Law of Neutrality provided the source of the due diligence standard breached by the United Kingdom in permitting ships to be built for the war effort on its territory. However, due diligence did not exist as a discrete requirement on states and indeed was simply a required standard of care when abiding by the Law of Neutrality. *See* Ala. Claims Arbitration (U.S. v. Gr. Brit.), 29 R.I.A.A. 125, 129 (1872). In addition, the applicability of the *Alabama* arbitration to any general obligation of due diligence is limited given that the *Alabama* arbitration was carried out pursuant to the Treaty of Washington of 1871, which itself provided for three "rules," two of which called for "due diligence" as the standard for assessing each state's conduct. *See generally* Treaty of Washington, Gr. Brit.-U.S., May 8, 1871, 17 Stat. 863.

interferences below a certain level of coercion are tolerated—or at least not clearly unlawful—as in the case of espionage.[172]

Yet even if we were to accept that a due diligence obligation attached to the principle of sovereignty, this approach would create significant conflicts with other legal constructs. For example, this approach would render the concept of intervention redundant; indeed, non-intervention might not make sense at all. After all, why would the prohibition on intervention be limited to coercive intrusions on a state's sovereign affairs if there already exists a duty of due diligence upon states to avoid *all* intrusions?

Though these differences might seem trivial, the consequences are not, especially in the context of low-intensity cyber attacks. For example, it is likely that states possess a due diligence obligation to prevent cyber attacks that constitute a use of force or intervention, since these are two categories where the primary duties prohibiting these acts may expressly incorporate a standard of due diligence.[173] However, it is less certain that due diligence attaches for cyber attacks below this level. For these attacks, one must turn to the relevant primary duty. In the case of low-intensity cyber attacks, this is the duty to prevent and redress transboundary harm. 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.[174]

---

172. *See supra* Section I.B.

173. *See* Sucharitkul, *supra* note 125, at 838. Still, uncertainty about this question persists.

174. It is unclear the extent to which the *Tallinn Manual* and Schmitt imply that due diligence applies in the low-intensity cyber context; however, several others offered such an argument. *See, e.g.*, Karine Bannelier-Christakis, *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyberspace?*, 14 BALTIC Y.B. INT'L L. 23 (2014); Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016). In fact, one could argue that Schmitt and the *Tallinn Manual* may have even implicitly invoked the concept of transboundary harm, perhaps out of concern that invoking sovereignty in too strict a sense might be problematic. After all, they seem to see due diligence as applying not to *all* intrusions into a state's sovereign territory, but instead to intrusions "inflict[ing] serious damage" or causing "adverse effects." TALLINN MANUAL, *supra* note 48, r. 5, cmt. 3, at 26; Schmitt, *supra* note 165, at 75. This suggests that most of the substance in the approach taken by Schmitt and the *Tallinn Manual* to due diligence may actually come through the words "damage," "effect," or "injury"—words that resonate strongly with the concepts explored by the ILC in its work on transboundary liability, and not necessarily with the concept of "sovereignty." That is, an invocation of the right to sovereignty alone, as compared to an invocation of transboundary harm, would struggle to draw a line between *any* intrusion and intrusions causing "serious damage."

This leads us to the next set of questions: how far liability for the duty to prevent transboundary harm extends and what standard of care it calls for. Despite relying on *Trail Smelter* and *Corfu Channel*, both Schmitt and the *Tallinn Manual* avoid addressing this set of questions.[175]

By only referencing due diligence, Schmitt and the *Tallinn Manual* avoid addressing whether states have an obligation not to launch cyber attacks outside of the context of non-intervention and use of force. When the duty is framed just in terms of due diligence, states appear to have only a positive duty to thwart other actors from using state territory to launch attacks. As the *Tallinn Manual* indicates, a state may not "allow knowingly its territory to be used for acts contrary to the rights of other States,"[176] and as such, "[s]tates are required under international law to take appropriate steps to protect those rights."[177] The *Tallinn Manual* goes so far as to suggest that due diligence applies to cyber attacks "launched from cyber infrastructure that is under the exclusive control of a government."[178]

Stepping back, these statements seem to be a relatively backwards way of getting at a more important idea: whether states owe not just positive duties to prevent attacks, but also negative duties to refrain from them. International law typically imposes a negative duty *not* to act in a certain way—such as a duty not to launch a cyber attack—before it imposes related positive duties to act—such as a duty to prevent others from launching a cyber attack. Accordingly, states are usually held responsible after violating not just positive duties but also negative duties.[179]

---

175. *See* TALLINN MANUAL, *supra* note 48, r. 5, cmt. 3, at 26 (discussing *Corfu Channel*); Schmitt, *supra* note 165, at 72 (discussing *Trail Smelter* and *Corfu Channel*).

176. TALLINN MANUAL, supra note 48, r. 5, cmt. 3, at 26 (quoting Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9)).

177. *Id.*

178. *Id.* cmt. 8, at 27-28.

179. For example, in human rights law, "first generation" human rights obligations are understood as obligations on states to refrain from certain behaviors. "Second generation" obligations include economic and social rights, which are often provided by the state. *See* CHRISTIAN TOMUSCHAT, HUMAN RIGHTS: BETWEEN IDEALISM AND REALISM 137-39 (3d ed. 2014).

Invoking liability for transboundary harm also helps resolve confusions that arise in the 2015 report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Despite commenting at length on the importance of the principle of sovereignty in cyberspace, this report does not provide a clear rule *against* states launching cyber attacks, though it recommends that "[s]tates should not knowingly *allow* their territory to be used for internationally wrongful acts." Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc.

B. Applicability to Low-Intensity State-Sponsored Cyber Attacks

I contend that (1) the relevant duty for low-intensity cyber attacks is the duty to prevent and redress transboundary harm and (2) this duty applies to *all* transboundary cyber harms above a minimum level of tolerance—including those that are intentionally caused by states. I propose associating the duty to prevent and redress transboundary harm with two standards of liability: absolute liability for attacks attributable to a state and due diligence for attacks by actors operating within a state's boundaries.[180] This dual-standard approach recognizes that positive and negative duties impose different burdens on states. While it is considerably more difficult for states to prevent non-state actors from launching an attack, states clearly have the ability *not* to launch attacks in the first place.

State-sponsored cyber attacks appear to meet the description of activities traditionally governed by absolute liability. Even the best-designed attacks carry a risk of damage to unintended parties, given the interconnectivity of the internet.[181] This militates in favor of considering state-sponsored cyber attacks to be essentially "abnormally" dangerous or "ultra-hazardous" activity for the purposes of liability.

A/70/174 (2015) (emphasis added). This formulation, like the due diligence formulations above, leaves unclear not only what such "internationally wrongful acts" might be, but also what duties states owe with respect to low-intensity cyber attacks in the first place.

180. "Within a state's boundaries" is taken broadly to apply to all non-state activities giving rise to cross-border harm, regardless of whether actors causing harm were physically present or acted via infrastructure located in a given state.

181. *See* McKay et al., *supra* note 38. *See generally* David Raymond et al., *A Control Measure Framework To Limit Collateral Damage and Propagation of Cyber Weapons*, NATO COOPERATIVE CYBER DEF. CTR. EXCELLENCE (2013), http://ccdcoe.org/cycon/2013/proceedings/d1r2s6_raymond.pdf [http://perma.cc/V8EE-4GRJ] (suggesting measures needed to prevent cyber weapons from causing indiscriminate harm). State-sponsored attacks may be more sophisticated than average non-state hacks, making them prone to significant destruction. *See, e.g.*, Kim Zetter, *Suite of Sophisticated Nation-State Attack Tools Found with Connection to Stuxnet*, WIRED (Feb. 16, 2015, 2:00 PM), http://www.wired.com/2015/02/kapersky-discovers-equation-group [http://perma.cc/CM86-PHHW].

FIGURE 3.
TWO STANDARDS OF LIABILITY FOR LOW-INTENSITY CYBER ATTACKS

	"Absolute" Liability	Due Diligence
Foundations in Domestic Tort & International Law	• Abnormally dangerous / ultra-hazardous activities • Activities with few societal benefits relative to costs • Activities for which the aim is total elimination or at least cost internalization • Often for *non-accidental* harms • "Common carrier" absolute liability • Intentional torts (with transferred intent, due care irrelevant)	• Harms resulting from activities with inherent societal benefits • Activities for which the costs of imposing absolute liability would unacceptably compromise other values • Activities for which resulting harms are foreseeable but preventable
Application to Low-Intensity Cyber Attacks	• Attacks attributed to states • Unprivileged state-sponsored "hack-backs" or unlawful countermeasures • Unintended harms to third parties	• Default standard when attribution to state cannot be made with confidence • Attacks attributed to non-state actors from within state territory • Attacks transmitted through internet or other infrastructure located on state territory (and not attributed to the state) • Harms resulting from foreseeable and preventable accidents resulting in serious trans-boundary cyber harms

The intentional nature of state-sponsored attacks supports absolute liability as the applicable standard of care, at least when attribution is possible. Typically, actors who commit intentional torts are liable for all directly consequent harms, regardless of the degree of care exercised or the extent to which the subsequent harms were foreseeable or intended.[182] For example, if a defendant intends to hit A and unintentionally hits B as well, the defendant is liable for damages caused to both A and B, even if the defendant was theoretically "diligent" in his or her attempt to hit A and not B.[183] This doctrine, known as the principle of transferred intent, imposes what amounts to absolute liability for

182. Lea Brilmayer explains, "Under international law, as in domestic law, foreseeability and proximate cause have been closely linked for both conceptual and practical reasons. Foreseeability is important as a convenient shorthand for the natural or probable consequences of any act." Lea Brilmayer, *Ownership or Use? Civilian Property Interests in International Humanitarian Law*, 49 HARV. INT'L L.J. 413, 442 (2008) Therefore, "[w]here harm is intentional, it is *necessarily reasonably foreseeable*, and foreseeability is generally sufficient *to satisfy the requirement of proximate cause*." *Id.* (emphasis added). The UN Compensation Commission has utilized this approach of substituting foreseeability for proximate cause. *See* Arthur W. Rovine & Grant Hanessian, *Toward a Foreseeability Approach to Causation Questions at the United Nations Compensation Commission, in* THE UNITED NATIONS COMPENSATION COMMISSION 235 (Richard B. Lillich ed., 1995).

183. This idea of absolute liability for intentional torts in international law finds support in the practice of the UN Compensation Commission. Though the Commission was only entitled under UN Security Council Resolution 687 to hold Iraq liable for "direct loss, damage . . . or injury," a Commission panel concluded that harms resulting from environmental pollution related to the burning of Kuwaiti oil wells were compensable. The panel found these harms sufficiently foreseeable and therefore proximate to merit compensation, in part because the burning of these fields was intentional. *See* Brilmayer, *supra* note 182, at 442. In addition, the *Draft Articles on State Responsibility* suggest that the intentional or deliberate nature of wrongful state actions can overcome the requirements of proximate cause when calculating reparations. *See* Draft Articles on State Responsibility, *supra* note 18, art. 31, cmt. 10, at 227-28 (emphasis added) ("[C]ausality in fact is a necessary but not a sufficient condition for reparation. There is a further element, associated with the exclusion of injury that is too 'remote' or 'consequential' to be the subject of reparation. In some cases, the criterion of 'directness' may be used, in others 'foreseeability' or 'proximity.' But other factors may also be relevant: for example, whether State organs *deliberately caused* the harm in question, or whether the harm caused was within the ambit of the rule which was breached, having regard to the purpose of that rule. In other words, the requirement of a causal link is not necessarily the same in relation to every breach of an international obligation."). In domestic law, the Third Restatement of Torts also provides for a broader scope of liability, through more expansive "proximate cause" limits, when an actor commits an intentional tort. RESTATEMENT (THIRD) OF TORTS: INTENTIONAL TORTS TO PERSONS § 110, cmt. a (AM. LAW INST., Tentative Draft No. 1, 2015).

intentional torts so as to discourage tortious conduct and to make whole each impacted party.[184]

By contrast, where attribution to a state is impossible, but attribution to private entities operating within a state's territory or via infrastructure located in a state *is* possible, an attack should only give rise to liability if the state failed to act diligently in preventing it. That is, the applicable standard of care imposed upon states in these cases should be due diligence. This obligation encourages states to take measures to prevent cyber criminals from operating within their territory. It also decreases the likelihood that states will escape liability for attacks that they launch but that are difficult to attribute to them, since due diligence will serve as the default standard of care. This approach is similar to the one proposed by Schmitt and the *Tallinn Manual*:

> [T]he due diligence principle . . . provide[s] grounds for a response when a state is suspected of engaging in the hostile cyber activities, but insufficient evidence exists to satisfy the level of certainty necessary for legal attribution. In other words, even where there is no smoking gun that would legally justify treating the cyber operations as those of the state, the state could be treated as having failed its due diligence obligation, and the principle would permit countermeasures on that basis.[185]

Yet in sharp contrast to the approach taken by the *Tallinn Manual*, a breach of the duty to prevent and redress transboundary harm should not give rise to state responsibility directly, but instead should result first in liability—that is, a requirement that the state compensate for the damages it caused. Liability, as opposed to responsibility, is particularly appropriate given the immense challenges of adequately assessing state actions,[186] as discussed in the next Part. This approach would also require states not simply to fire back countermeasures, but indeed to seek compensation through a liability claim before resorting to a claim that the attacking state should be held responsible.

---

184. One of the three driving points of the ILC's work on liability was the understanding that "an innocent victim should not be left to bear his loss or injury." Robert Q. Quentin-Baxter (Special Rapporteur), *Third Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, ¶ 53, U.N. Doc. A/CN.4/360 (June 23, 1982).

185. Schmitt, *supra* note 165, at 80. Rule 5 of the *Tallinn Manual* says that a state should not knowingly allow its infrastructure to be used to harm other states; the commentary to Rule 5 indicates that a state can violate Rule 5 absent a full finding of attribution. *See* TALLINN MANUAL, *supra* note 48, r. 5, cmt. 3, at 26.

186. *See* ILC Survey, *supra* note 84, ¶ 23 (noting the difficulty of assessing state conduct as "negligent").

In sum, the purpose of imposing either absolute liability or the due diligence standard of care should be to compel states to compensate for the damages caused by cyber attacks, as well as the damages caused by their inadequate monitoring and security of their domestic systems.

C. Complications of a Liability System

This Section considers potential issues with applying liability for transboundary harms to low-intensity cyber attacks, including whether the intentional nature of low-intensity cyber attacks prevents an application of liability, what level of damages can give rise to liability, and the mechanisms that might be invoked to impose liability.

1. The Issue of Intent

One might suggest that the duty to prevent and redress transboundary harm should turn on the issue of whether the state intended to cause the harm, but international law and precedent counsel otherwise. International tribunals have not held that intent precludes liability for the duty to prevent and redress transboundary harm.

For example, international law is often reluctant to pass judgment on the "mindset" of a state, particularly given uncertainty as to determining the intent of an expansive state apparatus.[187] In response to the puzzle of determining a state's "intent," effects-based assessments have gained prominence over the years. Under an effects-based assessment, a state may incur responsibility even when it unwittingly engages in certain prohibited or harmful activities.[188] The

---

187. In fact, the *Draft Articles on State Responsibility* explain that neither fault nor intention is necessary to find state responsibility. *See* Draft Articles on State Responsibility, *supra* note 18, art. 2, cmt. 10, at 73 ("[One] . . . question is whether fault constitutes a necessary element of the internationally wrongful act of a State. This is certainly not the case if by 'fault' one understands the existence, for example, of an intention to harm. In the absence of any specific requirement of a mental element in terms of the primary obligation, it is only the act of a State that matters, independently of any intention."). As it seems that the *Draft Articles on State Responsibility* do not require intent to find that state responsibility inheres, it is hard to explain (even at a theoretical level) why a finding of intent to harm would preclude application of international liability.

188. For example, in both the *Nicaragua* and *Armed Activities on the Territory of the Congo* cases, the "motive of the supporting State" in providing support to third parties was found to be "of little consequence," to a determination that the state had engaged in unlawful action. Watts, *supra* note 17, at 268-69; *see also* GRAY, *supra* note 43, at 79; HIGGINS, *supra* note 130, at 146-68.

UN International Group of Governmental Experts adopted such an "objective" approach for cyberspace, defining a cyber "armed attack" by the size and scale of damages involved, without reference to the state's "intent."[189]

If intent is not necessary in these cases, it would be unreasonable to require intent in the *low-intensity* cyber realm in order to hold a state liable for transboundary harm. After all, liability is less serious than responsibility, given that an injured state would make a liability claim against the attacking state before asserting that the attacking state should be held responsible,[190] and a liability claim does not permit injured states to take advantage of countermeasures, as responsibility frequently does.[191]

Perhaps the strongest argument for deeming intent irrelevant comes from the fact that a low-intensity attack is a per se negligent act, given the broader duty on states to prevent and redress transboundary harm. For example, the ILC conceives of the duty as encompassing a duty not only to perform risk assessments and to minimize risks of harm in prospective activities, but also to give notice and stop harm once the state becomes aware of it.[192] In this sense, once a state knows it is causing harm—even if it did not realize that its cross-border actions would do so at the outset—it has a duty to stop and redress the situation and to compensate injured parties for any harms caused.

International law has been quick to apply liability for "non-accidental" torts—that is, torts that are caused despite a state's awareness of harmful effects mounting over time.[193] In some senses, low-intensity state-sponsored cyber attacks resemble such "non-accidental" torts, and states are thus best held to a stricter standard of care—what I propose to be absolute liability—to be associated with the duty to prevent and redress transboundary harm.

---

189. Yoo, *supra* note 27, at 179-80. By contrast, according to Yoo, only a minority of the UN International Group of Governmental Experts refused to characterize instances like cyber espionage giving rise to unexpected and unintentional damages as an armed attack, even if damage otherwise amounted to the level of a traditional armed attack. *See id.* However, it should be noted that the *Tallinn Manual* suggests that the International Group of Governmental Experts could not come to clear agreement on whether a state could be held in breach of its due diligence obligations if it simply "should have known" about an impending attack. *See* TALLINN MANUAL, *supra* note 48, r. 5, cmt. 11, at 28.

190. *See supra* Section II.B.

191. *See* discussion *infra* Section IV.A.2.

192. *See* Draft Articles on Transboundary Harm, *supra* note 109, arts. 7-9, at 402-12.

193. *See* XUE, *supra* note 24, at 113-82.

2. Scale of Damages

Although a comprehensive discussion of damages and how courts should calculate them is beyond the scope of this Note, two issues merit attention here: whether liability can only be applied in the context of cyber attacks that result in physical damage and whether liability is likely to lead to claims that are too insignificant.

First, liability for the failure to prevent and redress transboundary harm need not be limited to instances of physical damage, so long as any nonphysical damage is of a degree not normally tolerated and not frivolous or trivial.[194] Domestic tort law includes many examples where liability for nuisance—a concept similar to the duty to prevent transboundary harms—has been applied to nonphysical territorial intrusions.[195] Similarly, international law has addressed nonphysical harm in disputes over radiation exposure from atmospheric weapon tests.[196]

Second, although some might be concerned about de minimis claims being brought, market forces are likely to dissuade plaintiffs from asserting claims that are unlikely to result in significant awards. Applying liability to the duty to prevent and redress transboundary harm would also deter de minimis claims, since a court would balance other societal considerations and equitable interests. Additionally, tort law and the concept of liability are more amenable than the doctrine of state responsibility to the idea of mitigation of damages, which would help limit the problem of unreasonably large claims. Unlike state responsibility, liability for transboundary harm is not concerned with per se vio-

---

194. *See id.* at 4, 7-8 (noting that transboundary liability requires a factual inquiry particular to the circumstances of each incident of whether the damages incurred were "greater than the mere nuisance or insignificant harm which is normally tolerated" by the international community (quoting Julio Barboza (Special Rapporteur), *Sixth Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, U.N. Doc. A/CN.4/428, annex (Mar. 15, 1990))). In addition, in the Iran-U.S. Claims Tribunal, compensation was provided even for lost profits and other "intangible" injuries to property owners. *See* Int'l Fin. Corp. v. Iran, 15 Iran-U.S. Cl. Trib. Rep. 189, ¶ 238 (1987); Sergey Ripinsky, Damnum Emergens *and* Lucrum Cessans *in Investment Arbitration: Entering Through the Back Door*, *in* INVESTMENT TREATY LAW 54 (Andrea K. Bjorklund et al. eds., 2009).

195. For example, noises, smells, and other intangible effects can constitute nuisances, given that one definition of nuisance is "interference" with another's enjoyment of his or her land. *See* ILC Survey, *supra* note 84, at 23.

196. *See* ILC Survey, *supra* note 84, at 79; *see also* Nuclear Tests (Austl. v. Fr.), Order, 1973 I.C.J. 99 (June 22).

lations of particular principles or prohibitions.[197] The *Draft Articles on Transboundary Harm* specifically call on states to cooperate in good faith to "minimi[ze] the effects of the risk."[198] When applying societal concerns and engaging an "equitable balance of interest" to determine liability, the *Draft Articles on Transboundary Harm* asks courts to weigh "the economic viability of the activity [causing harm] in relation to the costs of prevention demanded by the states likely to be affected."[199] Liability, in other words, entails a consideration of reasonable harm prevention by both parties.

Relatedly, liability for the duty to prevent and redress transboundary harm applies only to harms not encompassed by the practices of mitigation and prevention.[200] The *Draft Articles on Transboundary Harm* suggest that tribunals evaluating claims of transboundary harm consider "the degree to which the states likely to be affected are prepared to contribute to the costs of prevention," "the standards of protection which the states likely to be affected apply to the same or comparable activities," and any standards "applied in comparable regional or international practice."[201] This means that liability is less likely when applied to harms that have become routinely tolerated internationally, even if not accepted. Thus, cyber attacks that are considered routine acts of espionage would fall outside the scope of liability, since espionage has been tolerated by the international community for some time.

However, as global norms develop toward states reasonably protecting their infrastructure against cyber attacks, liability should not arise for harms to

197. León Castellanos-Jankiewicz, *Causation and International State Responsibility* 19 (Amsterdam Ctr. of Int'l Law Research Paper No. 2012-07), http://www.sharesproject.nl/wp-content/uploads/2012/01/Castellanos-Causation-and-International-State-Responsibility1.pdf [http://perma.cc/VEE4-MRJ8]; *see also* HIGGINS, *supra* note 130, at 163 (noting that responsible states may owe reparation for a breach of international law, even if no damage has resulted). The *Janes* claim provides some interesting insights into how liability should be conceived of at the damages stage. The Tribunal noted that damages should be calculated based on the harms suffered by the individuals involved in the dispute, not based on the amount of damage Mexico had theoretically caused to the United States through its violation of international law. This may provide a more concrete way to calculate damages than would be obvious under state responsibility, which would consider more theoretical costs, for example the cost of intrusion on a state's sovereignty. *See* Laura M.B. Janes (U.S. v. Mex.), 4 R.I.A.A. 82 (Gen. Claims Comm. 1925).

198. SHAW, *supra* note 117, at 861.

199. *Id.*

200. It should also be noted that in considering absolute liability specifically, the ILC did consider suggestions that damages for liability be limited. *See* ILC Survey, *supra* note 84, ¶ 223.

201. SHAW, *supra* note 117, at 862.

states that take unreasonably limited efforts to protect themselves.[202] For example, as Obama Administration's report on cyberspace stated, "[S]tates should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse."[203] But requiring only reasonable mitigation and prevention makes sense as states cannot possibly prevent all domestic cyber harms from foreign sources.

Although identifying the type of low-intensity cyber attack that would go beyond a state's baseline duty to protect itself is challenging, the State Department has made one threshold clear: North Korea's attack on Sony. In the words of one senior official, the Sony attack "clearly crossed a threshold" from "website defacement and digital graffiti" to an attack on IT infrastructure.[204] In the State Department's view, this attack fell beyond the bounds of reasonable mitigation and prevention, and thus should have given rise to state liability. While it may be too early to tell, some states seem willing to accept, or at least acquiesce to, this view.[205]

3. Enforcement

Though enforcement is always a challenge in international law, several characteristics of liability for transboundary harm make it a desirable way to regulate low-intensity cyber attacks: (1) diplomatic protection and settlement through *ex gratia* claims, (2) formal international legal claims, and (3) domestic suits under exemptions to foreign sovereign immunity. In this way, liability for transboundary harm proves effective for combating low-intensity cyber attacks, particularly in light of the alternatives discussed in Part IV.

Turning first to diplomatic protection, the history of international law is replete with examples of states taking action at the interstate level on behalf of citizens whose persons or property have been mistreated by another state. As

---

202. *See* Gross, *supra* note 165, at 498; David Fidler, *Cyber Norm Development and the Protection of Critical Infrastructure*, COUNCIL ON FOREIGN REL. (Jul. 23, 2015), http://blogs.cfr.org/cyber/2015/07/23/cyber-norm-development-and-the-protection-of-critical-infrastructure [http://perma.cc/7ZQG-7P7E].

203. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, WHITE HOUSE (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [http://perma.cc/R52L-Z556].

204. Sanger & Schmidt, *supra* note 51.

205. For example, China condemned the Sony attack, even though it disagreed that the attack could be definitively attributed to North Korea. *See* Megha Rajagopalan & Steve Holland, *China Condemns Cyberattacks, But Says No Proof North Korea Hacked Sony*, REUTERS (Dec. 22, 2014, 8:22 AM), http://www.reuters.com/article/us-sony-cybersecurity-idUSKBN0K006U20141222 [http://perma.cc/8GQ9-UQCR].

Emmerich de Vattel recognized in 1758, "[W]hoever ill-treats a citizen indirectly injures the State, which must protect that citizen."[206] Today, international investment law frequently deals with the issue of holding a state liable for harms caused to private actors. As the tribunal in *Mavrommatis Palestine Concession* explained, the act of a state taking up claims to "obtain satisfaction" on behalf of its subjects injured by or in a foreign state is an "elementary principle of international law."[207]

A state's espousal of a "claim of its citizen against the offending government" is known as "diplomatic protection."[208] For instance, diplomatic protection would involve a state asserting a claim on behalf of one of its nationals against a foreign state when the individual was harmed in the foreign state.[209]

In contrast to classical diplomatic protection, diplomatic protection for transboundary harms is in a sense "reverse" diplomatic protection: states make claims on behalf of their nationals who are injured *within their own borders* by foreign states, not outside of them. Indeed, states routinely make informal attempts at protection for harms to property or interests in their territories.[210] In

---

206. Draft Articles on Diplomatic Protection with Commentaries, art. 1 cmt. 3, Rep. of the Int'l Law Comm'n on the Work of its Fifty-Eighth Session, U.N. Doc. A/61/10, at 27 (2006) (quoting 3 EMMERICH DE VATTEL, THE LAW OF NATIONS OR THE PRINCIPLES OF NATURAL LAW APPLIED TO THE CONDUCT AND TO THE AFFAIRS OF NATIONS AND SOVEREIGNS 136 (C.G. Fenwick trans., Carnegie Inst. 1916) (1758))).

207. Mavrommatis Palestine Concession (Greece v. U.K.), Decision on Jurisdiction, 1924 P.C.I.J. (ser. A) No. 2, at 5, 12 (Aug. 30); *see also* Ahmadou Sadio Diallo (Guinea v. Dem. Rep. Congo), Preliminary Objections, Judgment, 2007 I.C.J. 582 (May 24); Paneveezys-Saldutiskis Railway (Est. v. Lith.), Judgment, 1939 P.C.I.J. (ser. A) No. 76, at 5, 6, 16 (Feb. 28) ("In the opinion of Court, the rule of international law . . . [at issue] is that in taking up the case of one of its nationals, by resorting to diplomatic action or international judicial proceedings on his behalf, a State is in reality asserting its own right, the right to ensure in the person of its nationals respect for the rules of international law.").

208. In these cases, states' claims have typically taken the form of an exchange of diplomatic notes. *See* BISHOP ET AL., *supra* note 137, at 2.

209. See *id.*

210. In the United States, the State Department has long been in the business of representing "citizen-to-state claims," that is "claims by U.S. citizens against foreign states and vice versa." Harold Hongju Koh, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1750 (2012). While in the early days, secretaries of state were known to use their diplomatic clout to espouse such claims before foreign governments, by the middle of the nineteenth century the practice had indeed become so common that it overwhelmed existing resources and prompted the creation of a new role of Claims Clerk. *See* Richard B. Bilder, *The Office of the Legal Adviser: The State Department Lawyer and Foreign Affairs*, 56 AM. J. INT'L L. 633, 634 (1962). The Office of the Legal Adviser of the State Department ultimately incorporated this role and to this day retains responsibility for managing various foreign claims. *See id.* at 634-38. In a related context, the Department of Justice

the context of transboundary harm, states have most frequently achieved such protection by negotiating claims of voluntary payments, also known as *ex gratia* payments in international law.[211]

Framing claims in international legal terms helps to create a common language on which to premise negotiation of voluntary settlements in the first place.[212] Tethering claims to underlying legal considerations may also encourage settlement by supplying legitimacy and lawful authority to states exercising diplomatic power.[213]

Ex gratia compensation may be particularly effective in the cyber context because it permits states to redress harms without having to acknowledge wrongdoing or causation. This can be useful when a state seeks redress for transboundary harms caused by a state that may be reluctant to acknowledge fault or causation. Such was the case when the United States, avoiding recognition of fault, compensated island nations harmed by nuclear weapons tests.[214]

In cases where voluntary compensation does not take place, international courts can provide an arena for hearing liability claims for violations of the duty to prevent and redress transboundary harm. The ICJ could provide a forum for formal claims of diplomatic protection for injuries caused to its citizens and private industries through low-intensity cyber attacks. In recent years, Argentina and Costa Rica have both invoked transboundary harm before the ICJ in the context of cross-border environmental damages.[215] In addition, states have made a variety of diplomatic protection-type claims before the ICJ on behalf of their nationals. In the *Diallo* case, for instance, Guinea sought relief for the vio-

adjudicates claims of U.S. nationals against foreign governments under specific jurisdiction conferred by Congress. Funds for the payment of awards are derived from congressional appropriations, international claims settlements, or the liquidation of foreign assets in the United States by the Department of the Treasury. *See About the Commission*, U.S. DEP'T JUST., http://www.justice.gov/fcsc/about-commission [http://perma.cc/5VYX-389W].

211. *See* Montjoie, *supra* note 105, at 512; *see also* ILC Survey, *supra* note 84, ¶¶ 405-411, 523; Jean-Marc Sorel, *The Concept of "Soft Responsibility?," in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 100, at 165 (discussing the relationship between liability and responsibility in the context of international law).

212. *See, e.g.*, Michael Waibel, *The Diplomatic Channel*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 100, at 1089-90.

213. *See id.* at 1091-92.

214. *See* ILC Survey, *supra* note 84.

215. Certain Activities Carried Out by Nicaragua in Border Area (Costa Rica v. Nicar.), Judgment, 2015 I.C.J. 1, ¶¶ 177-217 (Dec. 16); Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 18, ¶ 101 (Apr. 20).

lation of the human rights of its nationals by the Democratic Republic of the Congo.[216]

The Permanent Court of Arbitration could serve as another setting for settling transboundary harm claims stemming from low-intensity cyber attacks. Some states may be willing to submit to arbitration for even very contentious matters after some time has passed. Though states often refuse to proceed to arbitration (or even negotiations) immediately, changes in political circumstances may open up room for arbitration eventually. The unusual *Rainbow Warrior* case illustrates this phenomenon: France ultimately agreed to arbitration over damages resulting from its intelligence service blowing up a Greenpeace vessel.[217]

Finally, many governments have also recognized liability in their own courts for tort claims against foreign states. This could serve as an additional option for providing redress for low-intensity cyber attacks. Although foreign sovereign immunity may bar certain claims, customary international law on sovereign immunity may contain an exception for "territorial torts" committed by one state that affect another state's territory.[218] In fact, the UN Convention on Jurisdictional Immunities of States and Their Property has affirmed such a principle.[219] Guided by this logic, Greece has permitted suits against Germany for tortious injuries and damage sustained on Greek territory during World War II, and Italy has refused to recognize sovereign immunity as barring claims for similar tortious acts committed by Germany on Italian territory.[220]

---

216. *See* Ahmadou Sadio Diallo (Guinea v. Dem. Rep. Congo), Judgment, 2012 I.C.J. 324 (June 19); *see also* Barcelona Traction, Light & Power Co., Ltd. (Belg. v. Spain), Judgment, 1970 I.C.J. 3 (Feb. 5).

217. *See* Rainbow Warrior Affair (N.Z. v. Fr.), 11 R.I.A.A. 217 (1990); Geoffrey Palmer, Deputy Prime Minister of N.Z., Settlement of International Disputes: The "Rainbow Warrior" Affair, Address to the University of Virginia School of Law (Nov. 3, 1988), *in* 15 COMMONWEALTH L. BULL. 585 (1989).

218. *See* HAZEL FOX, G.C. & PHILIPPA WEBB, THE LAW OF STATE IMMUNITY 475-83 (3d ed. 2015). *But see* Jurisdictional Immunities of the State (Ger. v. It.), Judgment, 2012 I.C.J. 99 (Feb. 3).

219. *See* Convention on Jurisdictional Immunities of States and Their Property, art. 12, U.N. Doc. A/59/38 (Dec. 2, 2004) (not yet in force) ("[A] State cannot invoke immunity from jurisdiction before a court of another State which is otherwise competent in a proceeding which relates to pecuniary compensation for death or injury to the person, or damage to or loss of tangible property, caused by an act or omission which is alleged to be attributable to the State, if the act or omission occurred in whole or in part in the territory of that other State and if the author of the act or omission was present in that territory at the time of the act or omission.").

220. *See* Corte Cost., 22 ottobre 2014, n. 238, Foro it. 2015, I, 1152 (It.); Voitia v. Federal Republic of Germany [A.P.] [Supreme Court] 11/2000, p. 514 (Greece).

In the United States, the Foreign Sovereign Immunities Act explicitly codifies such an exception to sovereign immunity for torts carried out on U.S. territory—including for a wide variety of activities "in which money damages are sought against a foreign state for personal injury or death."[221] Relying on this exception, in *Letelier v. Republic of Chile*, a federal court denied sovereign immunity to Chile when Chilean officials detonated a car bomb in Washington, D.C., in 1976.[222] More recently, Congress has passed legislation that appears to broaden this exception and expand state liability to torts not entirely committed in the United States.[223]

In this way, recognizing transboundary liability would effectively open up two levels of redress: first, through liability—including claims heard either domestically or internationally—and, second, through international state responsibility in the event that attempts at compensation or settlement fail.[224]

IV. THE BENEFITS OF INTERNATIONAL LIABILITY

This final Part considers the theoretical and practical benefits of recognizing liability for low-intensity cyber attacks. Transboundary liability not only offers a practical solution to the gap for low-intensity cyber attacks but also avoids many of the downsides of an expansive use of traditional international legal concepts.

---

221. 28 U.S.C. § 1605(a)(5) (2012). The Canadian Constitutional Court has recognized a similar exception to sovereign immunity for territorial torts. Schreiber v. Canada (Attorney General), 2002 SCC 62 §§ 30-37. The European Convention on State Immunity has as well. European Convention on State Immunity art. 11, May 16, 1972, 74 E.T.S.

222. *See* De Letelier v. Republic of Chile, 748 F.2d 790, 792 (2d Cir. 1984); *see* Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RTS. L. REV. 227 (2015).

223. *See* Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2015). ("A foreign state shall not be immune from the jurisdiction of the courts of the United States in any case in which money damages are sought against a foreign state for physical injury to person or property or death occurring in the United States and caused by . . . (1) an act of international terrorism in the United States; and (2) a tortious act or acts of the foreign state . . . regardless where the tortious act or acts of the foreign state occurred."); *see also In re* Terrorist Attacks on September 11, 2001, 538 F.3d 71 (2d Cir. 2008) (explaining the "entire tort" requirement).

224. *See Liability for Injurious Consequences*, *supra* note 106, ¶ 41.

A. Pragmatic Appeal to States and Emphasis on Redress

Low-intensity state-sponsored cyber attacks address situations where states are unlikely to agree to constrain their activities by overtly declaring such attacks wrongful. Serious enough to cause costly damage, though not quite expansive enough to meet the scale of a use of force or intervention, these attacks are increasingly becoming a literal "nuisance" in international law. And yet, as states increasingly come to see low-intensity cyber attacks as a valuable option in their foreign policy toolkit,[225] it is difficult to imagine a world in which they will sign on to attempts to outlaw low-intensity cyber attacks completely, let alone accept the expansion of certain prohibitions (such as the use of force and intervention) to cover them. Liability for transboundary harm encourages states to internalize the costs of foreign harm associated with their cyber activities without requiring a new treaty or infringing upon other laws given its application only to acts otherwise not prohibited internationally.[226]

More importantly, there are persuasive reasons to resist declaring all low-intensity cyber attacks wrongful. As M.B. Akehurst explains, liability has several features that make it pragmatically preferable to responsibility:

> [A] certain stigma attaches to the commission of an unlawful act. States may therefore be reluctant to pay compensation for wrongful acts because they are unwilling to admit that they have done anything wrong. They may be more willing to pay compensation for lawful acts, because such payments do not imply a confession of wrongdoing. A rule requiring payment of compensation for lawful acts "should make easier a just, effective and amicable settlement of any liability that may arise."[227]

---

225. *See, e.g.*, *The Department of Defense Cyber Strategy*, U.S. DEP'T DEF. 14 (Apr. 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [http://perma.cc/U7GG-VHLF].

226. *See* ILC Survey, *supra* note 84, ch. 1. For a discussion of the need for international law to recognize civil liability for torts otherwise governed by international criminal law, see Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016).

227. Akehurst, *supra* note 114, at 15 (quoting Robert Q. Quentin-Baxter (Special Rapporteur), *Preliminary Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law*, ¶ 56, U.N. Doc. A/CN.4/334 (July 4, 1980)). It should be noted that the United States permits foreigners to bring tort suits against it under select statutes. *See, e.g.*, 10 U.S.C. § 2734(a) (2012); 28 U.S.C. § 1350 (2012). For example, by 2006, the United States had paid more than $26 million in compensation for tortious acts committed by U.S. soldiers in Iraq and Afghanistan under the U.S. Foreign Claims Act. *See* Jordan Walerstein, *Coping with Combat Claims: An Analysis of the Foreign Claim's Combat Exclusion*, 11 CARDOZO J. CONFLICT RESOL. 319, 339-40 (2009).

Moreover, the ILC has noted that accusations of wrongfulness may induce counterproductive antagonism instead of actual redress for injured parties.[228]

Greater antagonism would also result from taking any of the other approaches to addressing low-intensity cyber attacks. Expanding the definition of the use of force would allow states to label low-intensity cyber attacks as "armed attacks" and respond with force.[229] Even declaring all low-intensity cyber attacks just to be violations of non-intervention and sovereignty would permit states to take excessive countermeasures under state responsibility. Alternatively, subsuming low-intensity cyber attacks into the legally unclear category of espionage would require states to accept significant damage from foreign covert action and international law would remain unable to address it. Categorizing these sorts of attacks as espionage would also permit states to conduct in-kind low-intensity counter attacks, provided that these, too, stay at the level of cyber espionage. Either of these approaches would also fail to compensate for certain harms to private actors, such as the tens of millions of dollars in damages to companies like Sony.

Approaches invoking state responsibility would present their own concerns. For instance, holding states responsible for too many cyber attacks might encourage states to impose draconian restrictions on internet use. Moreover, expanding preexisting categories of law to proscribe low-intensity attacks could create havoc in areas of law unrelated to cyber attacks. And broadening the concept of intervention or sovereignty could result in severe problems for NGOs and other supporters of human rights who engage in what might be called low-level coercive activity.[230]

In addition, it is difficult to justify imposing state responsibility directly in cases where it is unclear whether an attack inadvertently passed through a state's borders due to the interconnectivity of the internet[231] or has been inaccurately attributed.[232] After all, responsibility is one of the most serious notions in international law and one that opens the door to ICJ and Security Council sanctions, outcasting, and remedies implicating a host of other legal rights and international obligations. Weakening or fundamentally altering state responsi-

---

228. *See Liability for Injurious Consequences*, *supra* note 106, ¶ 42.

229. The United States has long maintained that a violation of Article 2(4) triggers Article 51. *See* Koh, *supra* note 49, at 3-4.

230. *See* Hathaway, *supra* note 35, at 49 (noting that the gap between Article 2(4) and Article 51 "prevents an endless process of retaliations for small offenses").

231. *See* Michael N. Schmitt & M. Christopher Pitts, *Cyber Countermeasures and Effects on Third Parties: The International Legal Regime*, 14 BALTIC Y.B. INT'L L. 1, 2 (2015).

232. *See, e.g.*, Kenneth Geers, *The Challenge of Cyber Attack Deterrence*, 26 COMPUTER L. & SECURITY REV. 298, 301-02 (2010).

bility by creating a system that would be difficult to enforce or even comprehend in the cyber context would hardly be productive in the long term.[233]

In contrast, a liability approach, through its varying standards of care, can better account for low-intensity cyber attacks. Unlike an approach that invokes sovereignty or non-intervention, a dual liability regime provides a tailored approach to different cases depending on varying degrees of attribution. Similarly, liability takes into consideration varying degrees of reasonable conduct, particularly for attacks carried out by non-state actors via a state's infrastructure.[234] In addition, because liability works backwards from harm, as opposed to via an abstract principle for all breaches (intentional or not), it does not need to apply in all cases of theoretical injury to a state's sovereignty.[235] In this sense, liability supports a system where states are, even if not absolutely prohibited from launching attacks, at least compelled to account for damages and take reasonable steps to prevent cyber harms abroad.[236]

This proposed dual liability regime is even more attractive in light of another alternative: charging individual state officials or state-hired individuals for cyber harms (instead of states directly). For example, in March 2016, the United States indicted several Iranian state hackers for a range of cyber attacks on U.S. companies.[237] Critics have rightly pointed out that these indictments

---

233. Another problem with state responsibility, unlike liability, is that (at least in theory and according to the ILC) it is supposed to be concerned with *all* subjective violations of international law, even those that do not involve material damage. *See* Draft Articles on State Responsibility, *supra* note 18, art. 31, cmt. 7, at 92.

234. *See, e.g.*, Foster v. Preston Mill Co., 268 P.2d 645, 647-48 (Wash. 1954) (noting that tort law often limits the "defendant's duty to insure safety . . . to certain consequences" and compares damages with those experienced by neighbors (citations omitted)).

235. *See* ILC Survey, *supra* note 84, ¶ 27; *see also Foster*, 268 P.2d at 647 (describing the extent of liability incurred through ultrahazardous activities); Draft Articles on State Responsibility, *supra* note 18, arts. 30-31, at 216-31 (outlining the obligations of States responsible for "internationally wrongful act[s]"). In addition, and in some aspects paradoxically, traditional responsibility may actually require more substantial compensation than even "strict liability" does, since once responsibility is found, total reparation is required and is not likely to make any balancing approach. *See* BARBOZA, *supra* note 114, at 92.

236. Some experts have recently proposed a "cyber insurance" program, a cousin to the idea of state liability for cyber attacks. *See* Nathan Bruschi, *Maybe Wall Street Has the Solution to Stopping Cyber Attacks*, WIRED (June 2, 2016, 4:02 PM), http://www.wired.com/2016/06/cyber-bonds [http://perma.cc/3G3B-TY8G].

237. *See* Press Release, U.S. Attorney's Office for the S. Dist. of N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated [http://perma.cc/HD82-4V4V].

may set a problematic precedent for U.S. officials traveling abroad.[238] In certain cases, individual indictments can also divert attention away from the "true" source of liability: the state that actually ordered and developed the cyber attack in the first place. Even if a government could capture alleged cyber criminals, it would end up bypassing the party with "deeper pockets" that would be most able to change broad-ranging cyber policies.

B. Clarification of the Law of Countermeasures

Recognizing transboundary liability also elucidates the duties of states engaging in increasingly common "hack-backs," or what some refer to (sometimes incorrectly) as countermeasures.[239] According to the *Tallinn Manual*, "a State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[240] Countermeasures are nonviolent actions taken in response to another state's wrongful act[241] in order to induce compliance with international law.[242] However, under the *Draft Articles on State Responsibility*, countermeasures must be reversible "as far as possible,"[243] proportionate,[244] and can only be taken after demands for the cessation of the wrongful conduct fail.[245]

Recognizing the duty to prevent and redress transboundary harm and liability for low-intensity cyber attacks helps mitigate the problem of the overuse of cyber countermeasures, while at the same time not eliminating an important state tool. Liability requires states to seek settlement through compensation be-

---

238. *See, e.g.*, Robert M. Lee, *Feds Set a Risky Precedent by Indicting 7 Iranian Hackers*, WIRED (Mar. 26, 2016, 7:00 AM), http://www.wired.com/2016/03/feds-set-risky-precedent-indicting-7-iranian-hackers [http://perma.cc/8A4N-5DER].

239. *See, e.g.*, Schmitt, *supra* note 34, at 703; Schmitt & Pitts, *supra* note 231.

240. TALLINN MANUAL, *supra* note 48, r. 9, at 56.

241. *See* Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 3, ¶¶ 83-84 (Sept. 25).

242. *See* Draft Articles on State Responsibility, *supra* note 18, art. 49, at 328.

243. *Id.*

244. *See id.* art. 51, at 341; Air Servs. Agreement (Fr. v. U.S.), 18 R.I.A.A. 417, ¶ 83 (Dec. 9, 1978).

245. *See id.* art. 52, at 345; *Gabčíkovo-Nagymaros*, Judgment, 1997 I.C.J. ¶ 84. The law of countermeasures is reflected in customary international law. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 127, ¶ 248 (June 27); United States Diplomatic and Consular Staff in Tehran, Judgment, 1980 I.C.J. 3, ¶ 53 (May 24); Archer Daniels Midland Co. v. United Mexican States, ICSID Case No. ARB(AF)/04/5, Award, ¶ 124-25 (Nov. 21, 2007).

fore engaging in any countermeasure.[246] This requirement only amplifies what is already a condition inherent in the law of countermeasures: to first call on the state alleged to have caused harm to make reparations.[247] If compensation for transboundary harm is not provided after a significant period of de-escalation and recourse to domestic and international legal processes for settlement, then a state may be held responsible, and countermeasures may be considered, as at that point a wrongful international act would have been committed.[248]

FIGURE 4.

PERMISSIBLE INTERNATIONAL LEGAL RESPONSES FOR CYBER ATTACKS, INCLUDING UNDER A LIABILITY FRAMEWORK

Level of Attack	Possible Response
Armed attack	Self-defense (use of force)
Use of force short of "armed attack" & acts of intervention	Countermeasure (including attempts first at settlement)
Low-intensity attacks	Compensation or other settlement, and if not, potentially countermeasure

Another way of understanding the requirement to seek settlement before launching a countermeasure comes from the work of the ILC. The *Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities* indicate that "states are to co-operate in good faith in trying to prevent such activities from causing significant transboundary injury" as well as in mitigating the "effects of the risk," a notion that is also found in international environmental law.[249] The

246. *See* Hathaway, *supra* note 35, at 40-41, 46-47, 49. ("It is important that lawyers and policymakers be careful not to create bigger problems in other areas of international law when trying to solve the threshold problem in cyber by engaging in over-interpretation of broadly applicable legal principles."). It should also be noted that if the threshold for use of force is lowered to cover low-intensity cyber attacks, this effectively means that a state cannot respond *in kind* to such an attack through a countermeasure.

247. *See* Draft Articles on State Responsibility, *supra* note 18, art. 52, cmt. 1, at 345.

248. Analogous concerns in domestic law, particularly the need to maintain public order and prevent retaliatory self-help, drove the development of tort law and liability for breaches of particular duties. *See* ILC Survey, *supra* note 84, ¶ 18.

249. SHAW, *supra* note 117, at 861.

benefits of this approach may be particularly important when it comes to the cross-border effects that could stem from a range of different activities in contemporary society, not all of which could give rise to countermeasures under an expansive definition of sovereignty. These notions also square well with the UN Charter, which calls on "parties to any dispute . . . [to] first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement . . . or other peaceful means."[250]

C. Recognition of Duties Owed to Third Parties

Finally, applying liability for transboundary harms to low-intensity cyber attacks may clarify obligations owed to third-party states. Commentators have struggled to articulate the obligations—if any—that states have to third parties when engaging in countermeasures.[251] For instance, one line of analysis suggests that if a state launches a countermeasure against a second state and the countermeasure affects a third state, the third state has no recourse—unless the attack violates particular rights owed to that third state under a treaty.[252]

Recognizing the duty to prevent transboundary harm would affirm that liability fully extends to countermeasures affecting third parties. This is particularly important because cyber offenses are likely to cause unintended damages.[253] For instance, as the former head of the National Security Agency has recognized, unlike traditional weapons, malware and other cyber weapons do not self-destruct upon impact.[254] As a result, absent proper design, cyber

---

250. U.N. Charter art. 33; *see also* U.N. Charter art. 2(3) ("All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.").

251. *See e.g.*, Gross, *supra* note 165, at 501 n.123; Jay P. Kesan & Ruperto Majuca, *Optimal Hackback*, 84 CHI.-KENT L. REV. 831, 837 (2009); Schmitt & Pitts, *supra* note 231 at 6-8.

252. *See, e.g.*, Schmitt & Pitts, *supra* note 231, at 6-8 (distinguishing countermeasures that affect third party interests from those that affect third party rights, such as treaty rights).

253. *See* Raymond et al., *supra* note 181, at 8 (pointing out that Stuxnet was likely designed to target Iranian centrifuges at the Natanz uranium enrichment plant, but eventually infected systems in several countries); Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR (Mar. 2011), http://www.vanityfair.com/news/2011/03/stuxnet-201104 [http://perma.cc/6TLG-X79Y] (describing the spread of Stuxnet, a self-replicating computer virus, through thousands of computers around the world).

254. *See Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS (Jun. 4, 2012), http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012 [http://perma.cc/Z2KA-BDME]. For example, in the weeks following the alleged U.S. and Israeli Stuxnet attack on Iranian nuclear facilities, researchers identified the Stuxnet worm on hundreds of thousands of computers outside of Iran, in countries as disperse as Azerbaijan, the United Kingdom, India, Indonesia, Pakistan, and the United States.

weapons can effect repetitive damage that is far broader than intended. Liability is particularly equipped to deal with the problem of unintended consequences in cyber attacks. First, liability takes a somewhat less restrictive view of causation than responsibility.[255] Second, liability, especially an absolute liability standard, emphasizes that states have strict duties to prevent *all* low-intensity harms to third states, regardless of whether the state launching the attack "took care" to guard against such third-party harms or intended to hit only one target.[256]

Recognizing liability for damages to third parties resulting from illegal hack-backs or lawful countermeasures also sheds light on another unresolved issue in the literature: whether states have a right to property in international law, and thus a right not to have their property or property in their territory damaged.[257] While not answering the question directly, liability for transboundary harm suggests that low-level torts and cross-border property damages are not without limitation or redress in international law simply because they occur outside of armed conflict, intervention, or the use of force.

CONCLUSION

Liability for the duty to prevent and redress transboundary harm can fill the gap in public international law for low-intensity cyber attacks. States are not only subject to the standard of due diligence in preventing transboundary cyber harms originating from non-state sources, but also subject to absolute liability in terms of refraining from causing harm through attacks themselves—even when these attacks are not otherwise outlawed directly.

Jarrad Shearer, *W32.Stuxnet,* SYMANTEC (July 13, 2010), http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 [http://perma.cc/9L35-ARNG]. This resulted in fear that the malware would "bring industrial society to a halt," given that the worm targeted programmable-logic controllers common to many industries (e.g., oil extraction, dams, energy production, water distribution, and aviation). Gross, *supra* note 253.

255. *See* Castellanos-Jankiewicz, *supra* note 197, at 52 (noting that responsibility tends to adhere to proximate causation over direct causation); ILC Survey, *supra* note 84, ¶ 25.

256. *See* Brilmayer, *supra* note 182, at 442. Taken from another perspective, recognizing the duty to prevent transboundary harm to third parties simply applies notions of precaution owed under *other* bodies of law, such as the Laws of Armed Conflict (e.g., the principles of distinction and proportionality), to the low-intensity cyber realm. State practice also seems to support recognition of liability to third states, given that many state cyber weapons are carefully designed to attack precisely one target and to avoid replication outside of target environments.

257. *See* John G. Sprankling, *The Global Right to Property*, 52 COLUM. J. TRANSNAT'L L. 464, 491-97 (2014); Peter Tzeng, Comment, *The State's Right to Property Under International Law*, 125 YALE L.J. 1805 (2016).

Thus, I argue for an approach that avoids both expanding preexisting categories of wrongful state action and leaving all low-intensity cyber attacks outside of the fold of international law entirely. Liability for the duty to prevent transboundary harm not only encourages peaceful settlement and de-escalation, but also offers a more realistic approach for addressing the cross-border intrusions that are becoming increasingly common in the contemporary era.