TEACHING OLD LAW NEW TRICKS: APPLYING AND ADAPTING STATE RESPONSIBILITY TO CYBER OPERATIONS

by
Thomas Payne[*]

Transnational cyber operations are an immediate concern to scholars and practitioners of international law. Much scholarly work addresses the applicability of the jus ad bellum and jus in bello—the law of armed conflict—to cyber operations. This Comment addresses cyber operations through the "peacetime" framework of state responsibility for internationally wrongful acts. While cyber-specific international legal norms will certainly emerge, existing international law also applies to the cyber context. After first providing a general overview of the sources and types of public international law, this Comment explores which international legal norms a cyber operation might violate and the problem of attribution of cyber operations to states. This Comment also assesses the risk of privatizing or delegating cyber defense. Finally, this Comment concludes that existing international law has certain specific gaps, which would be well-addressed through new customary or conventional norms.

[*] J.D., 2016, Lewis & Clark Law School; B.A. Ed., 2011, University of Portland. The author would like to thank the staff of *Lewis & Clark Law Review* for their helpful editorial insights, particularly Nicholas Lauren, Michael Beilstein, and Elli Reuland. The author would also like to thank Dagmar Butte for her guidance and feedback while writing this Comment—and for getting him hooked on international law through the Phillip C. Jessup International Law Moot Court Competition. Finally, the author expresses his sincere gratitude to his wife, Sarah Khatib, for her unwavering support.

I. INTRODUCTION

In November of 2014, a previously unknown group calling itself the "Guardians of Peace" breached protected computer networks of Sony Pictures Entertainment, stealing data and disabling computer systems.[1] Computer security experts and investigators suggested that the Democratic People's Republic of Korea ("DPRK" or "North Korea") was behind the breach because of certain features in the code used in the attack and Sony's impending release of *The Interview*, a film about killing Kim Jong Un, the leader of the DPRK.[2] Shortly after U.S. President Barack Obama publically blamed North Korea for the breach and pledged a proportional response, North Korea's internet suffered widespread, catastrophic outages without explanation. One can only assume these outages were due to an American cyber operation.[3]

More broadly, cyber operations are an urgent concern for the international community because individuals and groups now have the potential (through cyber operations) to cause damage with the severity and scope historically limited to States—including the potential for mass destruction.[4] Despite the specter of terrorists striking with radiological weapons, chemical agents, and biological agents, weapons of mass destruction—especially in their most dangerous forms—remain largely in the possession of States.[5] However, today's automated and computerized

---

[1] Nicole Perlroth, *Sony Pictures Computers Down for a Second Day After Network Breach*, N.Y. TIMES (Nov. 25, 2014), http://nyti.ms/1rqG4ln.

[2] Jim Finkle, *North Korea Surfaces in Sony Investigators' Probe into Hack*, REUTERS (Dec. 4, 2014), http://www.reuters.com/article/us-sony-cybersecurity-investigation-nkor-idUSKCN0JH28920141204. Like many cyber operations, attributing this action to any particular country, let alone specific persons or groups within a country, is a significant challenge. *See* Nicole Perlroth, *New Study May Add to Skepticism Among Security Experts that North Korea Was Behind Sony Hack*, N.Y. TIMES (Dec. 24, 2014), http://nyti.ms/1CDFb2g.

[3] *See North Korean Websites Back Online After Shutdown*, TIMES-PICAYUNE (Dec. 22, 2014), http://www.nola.com/science/index.ssf/2014/12/north_korean_websites_back_onl.html; David E. Sanger, Michael S. Schmidt & Nicole Perlroth, *Obama Vows a Response to Cyberattack on Sony*, N.Y. TIMES (Dec. 19, 2014), http://nyti.ms/1v0KOi9.

[4] Cyber operations could, in theory, cause a nuclear power plant to meltdown, or goad a State into launching nuclear weapons. This possibility for cyber operations to cause mass destruction is remote, though. Brian Palmer, *How Dangerous Is a Cyberattack?*, SLATE (Apr. 27, 2012), http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html.

[5] Chemical, biological, and nuclear weapons are most often used by the military of a State, but are occasionally used by non-State actors. *Compare Cloud of Chlorine Borne by a Favoring Wind Germany's Novel Weapon that Swept Allies' Front; Was Released from Bottles of the Liquefied Gas*, N.Y. TIMES, Apr. 26, 1915, at A1, *and Congressmen Reveal Germ Weapon Can Wipe Out City at Single Blow*, N.Y. TIMES, May 25, 1946, at A1, *and*

world leaves the potential for mass destruction within the grasp of far less sophisticated actors and organizations—by engaging in computer network attacks commonly known as cyber operations.[6]

The Sony incident represents an interesting grey area in international law—unfriendly, damaging cyber operations that nonetheless exist in a relatively peaceful context. Voluminous scholarship addresses "cyber warfare" and application of the *jus ad bellum* and *jus in bello* (collectively, the law of war) to cyber operations.[7] But the Sony incident did not spark armed conflict. This apparent attack and counter-attack in peacetime[8] highlights the importance of applying the framework of state responsibility to cyber operations, holding states accountable for hostile cyber operations outside of armed conflict. The law of state responsibility governs the international responsibility of states for acts contrary to international legal norms.[9] This Comment will refer to hostile acts using computer

---

Sidney Shalett, *New Age Ushered*, N.Y. TIMES, Aug. 7, 1945, at A1, *with* C.J. Chivers, *ISIS Has First Chemical Mortar Shells, Evidence Indicates*, N.Y. TIMES (July 17, 2015), http://nyti.ms/1CMZDiJ, *and* Nicholas D. Kristof, *Hundreds in Japan Hunt Gas Attackers After 8 Die*, N.Y. TIMES, Mar. 21, 1995, at A1, *and* Sandra Sobieraj, *White House Mail Machine Has Anthrax*, WASH. POST (Oct. 23, 2001), http://www.washingtonpost.com/wp-srv/aponline/20011023/aponline201158_000.htm. Sophisticated high-yield nuclear weapons and large quantities of chemical and biological weapons are still exclusively possessed by States. *See generally Nuclear Forces Guide*, FED'N AM. SCIENTISTS, http://fas.org/nuke/guide/index.html (linking to general overviews of the nuclear, chemical, and biological weapons capacity of States).

[6] *See generally* William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INT'L L. STUD. 387 (2013) (discussing the various mechanisms of military cyber operations). Networked infrastructure is a commonly discussed target. Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 826–27 (2012) (detailing potential targets of destructive cyber operations). A cyber operation could target communications and electrical infrastructure, for example. Palmer, *supra* note 4.

[7] *See, e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]; Boothby, supra note 6. An important contribution to the delineation of States' peacetime obligations in the cyber context is a recent collection of essays, published by the same organization that produced the Tallinn Manual. PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE (Katharina Ziolkowski ed., 2013).

[8] Of course, the Korean War ended in an armistice agreement, not a formal peace treaty. *See* Agreement Between the Commander-In-Chief, United Nations Command, on the One Hand, and the Supreme Commander of the Korean People's Army and the Commander of the Chinese People's Volunteers, on the Other Hand, Concerning a Military Armistice in Korea, July 27, 1953, 47 A.J.I.L. SUPP. 186.

[9] *See* Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, U.N. GAOR, 53rd Sess., U.N. Doc. A/56/10, art. 2 (2001) [hereinafter Articles on State Responsibility]. This inquiry begins with a simple foundation: "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and

networks as "cyber operations," to emphasize the breadth of potential hostile acts short of all-out warfare.[10] To illustrate that breadth, cyber operations can range from unsophisticated DoS attacks[11] to costly data breaches[12] to starting a nuclear war.[13] In consideration of that breadth,

---

(b) constitutes a breach of an international obligation of the State." *Id.* For a comprehensive discussion of the international law applicable to cyber operations and cyber warfare, see the TALLINN MANUAL, *supra* note 7. The Tallinn Manual—developed by a NATO-sponsored group of experts—comprehensively explores the international law applicable to cyber warfare and proposes a normative framework for cyber operations based primarily on existing customary rules. This Comment will focus on state responsibility for individual cyber operations, discussed in Rules 1 to 17 of the Tallinn Manual.

[10] Scholars and practitioners use a variety of terminology to discuss computer network attacks. *See, e.g.*, TALLINN MANUAL, *supra* note 7, at 16; Lotrionte, *supra* note 6, at 826; Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 571 (2011). In news articles and common parlance, "cyberattack" is more common. *See, e.g.*, Sanger et. al, *supra* note 3.

[11] A DoS, or Denial of Service, attack uses a high number of packet requests (digital information requests from a website) to disrupt a website's functionality for a period of time. Mindi McDowell, *Security Tip (ST04-015): Understanding Denial of Service Attacks*, U.S. COMPUT. EMERGENCY READINESS TEAM (Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/ST04-015. DoS attacks are relatively cheap and unsophisticated, but do not cause significant amounts of damage. An example of a DoS attack is the 2011 attack by a hacker group on the CIA's website. Matthew J. Schwartz, *LulzSec Claims Credit for CIA Site Takedown*, INFORMATIONWEEK (June 16, 2011), http://www.informationweek.com/government/cybersecurity/lulzsec-claims-credit-for-cia-site-takedown/d/d-id/1098340?; *see also* Randall Munroe, *CIA*, XKCD, https://xkcd.com/932/ (illustrating the relatively insignificant effects of an average DoS attack: "Someone tore down a poster hung up by the CIA!!"). However, large-scale DoS attacks, such as the 2007 attacks on a number of Estonian government websites, can cause significant disruption in the operations of a State's governmental functions. Schmitt, *supra* note 10, at 570 ("The impact of the [2007 cyber operation on Estonia] proved dramatic; government activities such as the provision of state benefits and the collection of taxes ground to a halt, private and public communications were disrupted, and confidence in the economy plummeted."). For a more detailed explanation of the incident and its consequences, see ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 15–32 (2010).

[12] Data breaches can target the personal information of individuals, proprietary information, or any other confidential information. See the discussion of the Sony Pictures hack, *supra* notes 1–2 and accompanying text; *see also* David Alexander, *Theft of F-35 Design Data Is Helping U.S. Adversaries—Pentagon*, REUTERS (June 19, 2013), http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619 (discussing Chinese cyber espionage targeting Lockheed Martin and other defense contractors); Robert Hackett, *Massive Federal Data Breach Affects 7% of Americans*, TIME (July 9, 2015), http://time.com/3952071/opm-data-breach-federal-employees/ (discussing a data breach at the Office of Personnel Management, exposing personal information of federal employees as well as security clearance information).

[13] *See* Palmer, *supra* note 4. This possibility is quite attenuated.

this Comment seeks to explore state responsibility for cyberattacks beyond the well-studied realm of the use of force.

This Comment explores issues of state responsibility for transnational cyber operations in three main parts. The remainder of Part I will provide an overview of types of cyber operations and of the public international law framework, as a foundation for the discussion of state responsibility for cyber operations. For those unfamiliar with cyber operations or international law—or both—this overview provides context for understanding the remaining discussion. Part II will discuss the issue of state responsibility for transnational cyber operations committed by organs of a State. Because the actions of the organs of a State are essentially those of the State, discussion of cyber operations attributable to the organs of a State allows a general consideration of the international obligations implicated in cyber operations. Part III will focus on state responsibility committed by non-State actors for actions. When possible, this discussion will use structures and mechanisms hypothesized to exist in China and Russia to apply the principles of state responsibility to potential scenarios. Part IV will explore the potential ramifications of a counterattack by a private actor following an attack by a State actor, using a counter-factual version of the 2014 Sony incident.

A. An Overview of Public International Law

Public international law is the legal framework for the interactions of States within the international community.[14] In comparison to American domestic law, public international law has a number of unique and unfamiliar characteristics. The international community has no constitutional law-making body, unlike the legislatures and parliaments of individual States.[15] Instead, the legal rights and obligations of States are based on the "common consent" of States.[16] Consent to be bound by a principle of law may be found in actual consent, such as in signing a treaty, or in implied consent, through membership in the international community.[17]

---

[14] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 15–16 (8th ed. 2012); 1 OPPENHEIM'S INTERNATIONAL LAW 4 (Robert Jennings & Arthur Watts eds., 9th ed. 1992); MALCOLM N. SHAW, INTERNATIONAL LAW 5–6 (5th ed. 2003).

[15] CRAWFORD, *supra* note 14, at 20.

[16] OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 14–16.

[17] This implied consent gives rise to the generally applicable body of customary law. Through a sort of international social contract, States consent to be bound by the body of law as a member of the international community—even when a particular rule is unfavorable to a State, the body of law as a whole benefits the State as a member of the community of States. *See* CRAWFORD, *supra* note 14, at 7.

> The common consent that is meant is thus not consent to particular rules but to the express or tacit consent of states to the body of rules comprising international law as a whole at any particular time. Membership of the international community carries with it the duty to submit to the existing body of

However a State consents to be bound, its rights and obligations flow from a variety of sources. In discussing the sources of international law, this Section will loosely follow the format used in the Statute of the International Court of Justice.[18]

The legal rights and obligations of States flow from three primary sources of law: treaties, custom, and general principles of law.[19] Treaties are the most authoritative source of law, representing the affirmative consent of the signatories to be bound by certain obligations.[20] Treaties are clearly binding on the signatories of the treaty, but are only relevant to non-signatories if the rules created therein become custom.[21] Custom is the unwritten body of law formed by rules with which states comply out of a sense of legal obligation. Custom is shown by (1) uniform and widespread State practice complying with a rule, and (2) *opinio juris*, a sense

---

> such rules, and the right to contribute to their modification or development in accordance with the prevailing rules for such processes . . . .
>
> [N]o [S]tate can at some time or another declare that it will in the future no longer submit to a certain recognised rule of international law. The body of the rules of this law can be altered by the generally agreed procedures only, not by a unilateral declaration on the part of one state. This applies to all rules other than those created by treaties which admit of denunciation or withdrawal.

OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 14–15.

[18] "Historically the most important attempt to specify the sources of international law was Article 38 of the Statute of the Permanent Court of International Justice [the League of Nations predecessor of the ICJ], taken over nearly verbatim as Article 38 of the Statute of the International Court of Justice." CRAWFORD, *supra* note 14, at 21–22 (footnote omitted). The relevant portion of the Statute of the International Court of Justice is as follows:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

Statute of the International Court of Justice art. 38, ¶ 1.

[19] Statute of the International Court of Justice art. 38, ¶ 1 (a)–(c); CRAWFORD, *supra* note 14, at 20–21; OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 24.

[20] CRAWFORD, *supra* note 14, at 21, 30.

[21] OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 32. For a rule found in a treaty to crystalize into custom, both signatories and non-signatories must comply with the rule out of a sense of legal obligation. *See* North Sea Continental Shelf (Ger./Den., Ger./Neth.), Judgment, 1969 I.C.J. 3, ¶¶ 63–81 (Feb. 20) (deciding that the Convention on the Continental Shelf had neither created nor codified a customary norm regarding delimitation of boundaries on the continental shelf).

of legal obligation to comply with that rule.[22] Because these rules change, custom is not static, but an evolving body of rules that grows to accommodate changed circumstances and new challenges (such as cyber operations).[23] Thus, when a new situation arises, such as the digital revolution, showing custom is challenging because State practice is limited to a relatively brief period. The shorter duration of State practice requires more extensive and uniform practice, consistent with the sense of legal obligation.[24] Finally, general principles of law are less well-defined sources of law, referring both to near-universally accepted principles found in domestic law and undisputed abstract principles of international law that cannot be shown through State practice.[25] A commonly used general principle is the presumption of good faith, which is found in the U.N. Charter but applied generally in international law.[26]

---

[22] *North Sea Continental Shelf*, 1969 I.C.J. ¶ 77; CRAWFORD, *supra* note 14, at 25–26; OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 25–31; SHAW, *supra* note 14, at 69–88.

[23] Custom recognizes the consensus of States on their unwritten legal obligations—which can change as State opinion and practice changes. CRAWFORD, *supra* note 14, at 23–24. This change is more likely to be additive than subtractive. *See id.* at 24.

[24] Custom is subject to change, but how fast that change can occur is not a settled subject. *Compare* CRAWFORD, *supra* note 14, at 24 ("[T]he formation of a customary rule requires no particular duration . . . . [R]ules relating to airspace and the continental shelf have emerged following a fairly quick maturation period."), *with* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 30 ("[U]sually customary law is too slow a means of adapting the law to fast-changing circumstances."). The ICJ's approach, as set out in the *Continental Shelf* opinion, supports a more rigorous analysis for fast-emerging custom. *See* 1969 I.C.J. ¶ 74.

> Although the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule, an indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; —and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved.

Id. Essentially, the ICJ does not foreclose the possibility of fast-emerging custom, but requires a more rigorous showing of State practice and *opinio juris* when State practice is relatively recent.

[25] CRAWFORD, *supra* note 14, at 34–35; OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 36–40. General principles are a less-commonly used source of law, but they provide a helpful source of law to "fill gaps or weaknesses in the law which might otherwise be left by the operation of custom and treaty, and provide[] a background of legal principles in the light of which custom and treaties have to be applied." *Id.* at 40 (footnote omitted).

[26] OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 38 (citing U.N. Charter art. 2, ¶ 2); *accord* CRAWFORD, *supra* note 14, at 36; SHAW, *supra* note 14, at 98.

Custom and general principles are unwritten sources of law, in contrast to the text of a treaty.[27] Because custom and general principles are unwritten—and because no international body can create universally binding law—secondary sources of law are important as evidence of custom and general principles.[28] Judicial decisions and the writings of noted publicists can both show and clarify custom and general principles.[29] In international law, judicial decisions do not create binding precedent; instead, previous decisions are persuasive as evidence of the law.[30] Decisions of the International Court of Justice (ICJ) are usually persuasive to the Court and to other tribunals.[31] While all arbitral decisions are a potential source of law, some arbitral decisions are more persuasive than others—cases such as *Trail Smelter* are widely regarded, as are tribunals such as the Iran–United States Claims Tribunal.[32] Especially where cases cannot clarify a point of law, the writings of publicists are a subsidiary source of international law. An international legal scholar's persuasiveness depends on the authority and expertise of the scholar in a particular area.[33] The work of the International Law Commission, a group of well-regarded publicists, is especially persuasive.[34] The Commission's efforts to codify areas of international law have been generally cited with approval by the ICJ.[35]

---

[27] *See, e.g.*, Statute of the International Court of Justice art. 38, ¶ 1(d) (characterizing "judicial decisions and the teachings of the most highly qualified publicists of the various nations" as "subsidiary means for the determination of rules of law").

[28] Authors play an important role in ordering and structuring existing rules. SHAW, *supra* note 14, at 106. Scholars can also contextualize the acts of States. *Opinio juris*, for example, can be inferred by scholarly consensus. CRAWFORD, *supra* note 14, at 26.

[29] In the context of international law, "publicist" refers to "scholars of both public and private international law." BLACK'S LAW DICTIONARY (10th ed. 2014).

[30] "Since judges do not in principle make law but apply existing law, their role is inevitably secondary since the law they propound has some antecedent source." OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 41.

[31] In the interest of consistency, the ICJ is especially deferential to past opinions. *See* CRAWFORD, *supra* note 14, at 26; OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 41.

[32] These sources are cited as examples; many cases and tribunals have prominent status as evidence of the law. CRAWFORD, *supra* note 14, at 39–40, 353.

[33] Courts rarely cite noted publicists in opinions. Whether that shows the collaborative process of writing a majority opinion or the coming obsolescence of publicists is a subject of debate. *See* CRAWFORD, *supra* note 14, at 43; OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 42–43.

[34] CRAWFORD, *supra* note 14, at 43–44; SHAW, *supra* note 14, at 113–14 ("[I]t is not to be overlooked that the International Law Commission is a body composed of eminently qualified publicists . . . .").

[35] SHAW, *supra* note 14, at 113. For example, the International Law Commission's work in codifying the law of international responsibility, which culminated in the

Finally, the mechanism of State responsibility merits introduction. State responsibility for an internationally wrongful act requires a breach of an obligation of the State that is attributable to the State.[36] State responsibility for the acts of the State itself—through its organs and governmental units—is well established under international law.[37] State responsibility for the acts of private entities that the State directs or controls is equally uncontroversial.[38] When the wrongful acts of private entities are not attributable to the State, a State has some obligations to respond to wrongful acts taken by its citizens.[39] In any event, it is important to remember that a wrongful act must somehow relate to the acts or omissions of the State to create State responsibility.

B. An Overview of Cyber Operations

This Section establishes a common vocabulary for different types of cyber operations that is used throughout the Comment. As a note of caution, this Comment is written to explore the applicable law, not the underlying computer science. Accordingly, its approach is likely simplistic from a technical perspective. "Cyber operation" will be used as a catchall for any computer-network attack or computer-based action.[40] This broad term is intended to encompass any unwelcome act using computer code.

"DoS" will refer to a denial of service attack, which uses packet requests to overwhelm a server and render it inoperable.[41] If successful, this type of attack disables the functionality of a website or other computer network service. DoS attacks do not create lasting damage to the server or other network infrastructure. A subset of DoS attacks is a "DDoS" attack, which stands for distributed denial of service.[42] DoS and DDoS attacks do not require much technical sophistication to deploy.

Articles on Responsibility of States for Internationally Wrongful Acts, has "been relied on extensively by international courts and tribunals as an authoritative statement of the law on state responsibility." CRAWFORD, *supra* note 14, at 44; *see, e.g.*, Gabcíkovo-Nagymaros (Hung./Slovk.), Judgment, 1997 I.C.J. 7, ¶¶ 47, 50, 79, 83, 132 (Sept. 25) (citing the Articles on State Responsibility).

[36] Articles on State Responsibility, *supra* note 9, arts. 1–2.

[37] Brigitte Stern, *The Elements of an Internationally Wrongful Act*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 193, 203 (James Crawford, Alain Pellet & Simon Olleson eds., 2010).

[38] *Id.* at 206.

[39] *Id.* at 208–09.

[40] See *supra* note 10 and accompanying text for discussion of varying terminology for computer network attacks.

[41] See *supra* note 11 for a general discussion of DoS attacks.

[42] DDoS attacks use a network of personal computers to send enough packet requests to overwhelm a server. McDowell, *supra* note 11. Often, these personal computers have been compromised by malware, and their owners are unaware that they are being used as part of a cyber operation. *See id.*

"Malware" will refer to any computer program intended to act without a user's intent or permission. These programs include, without limitation: viruses, Trojan horses, worms, keyloggers, and ransomware.

"Network intrusion" will refer to a broad variety of techniques with the same effect: unauthorized access into a secure network. This can be achieved through password theft, malware, or other software exploits. This term applies regardless of the network intrusion's intended result. Though network intrusions have many purposes, they can be used to acquire confidential data or communications, monitor computer activity, and introduce malware into a network.

"Infrastructure-interference operation" will refer to any cyber operation that affects physical infrastructure, whether it disables or destroys that infrastructure. For example, a network intrusion used to shut down a power plant or disable a radar station would be an infrastructure-targeted attack. "Infrastructure-damaging operation," a subset of infrastructure-interference operation, will refer to a cyber operation that damages physical infrastructure. An example of an infrastructure-damaging attack is the Stuxnet/Olympic Games attack against Iran, which used malware to over-accelerate and destroy uranium centrifuges.[43]

II. STATE RESPONSIBILITY FOR CYBER OPERATIONS COMMITTED BY ORGANS OF THE STATE

This Part will explore when a cyber operation committed by an organ of a state, such as the military or secret intelligence agency, or a State-controlled entity such as a State-owned company, is an internationally wrongful act. For clarity, this Comment will refer to cyber operations committed by State organs and State-controlled entities as "State cyber operations." In contrast, this Comment will refer to cyber operations committed by entities not part of the state (e.g., groups temporarily controlled or directed by a State, "patriotic" hacker groups not controlled by a State, and criminal/terrorist hacker groups) as "non-State cyber operations." First, Section II.A will analyze when State cyber operations violate a State's international legal obligations. This Section will consider the impact of specific methods and targets, using real-world examples when possible. Then, Section II.B will briefly explain when the conduct of public entities (both organs of a State and State-controlled entities) is attributable to a State under international law.

[43] Gary D. Brown & Andrew O. Metcalf, *Easier Said than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 115 (2014).

A. International Obligations Implicated by State Cyber Operations

A cyber operation may violate a number of international obligations. This Section will assess obligations arising under customary international law but will not explore conventional obligations other than the United Nations Charter. First, various types of cyber operations may violate the prohibition on the use of force. In considering the issue of use of force, this Section will use the analytical framework proposed in the Tallinn Manual, which applies existing conventional and customary principles to cyber operations.[44] Second, cyber operations may violate the principle of non-intervention. While the law of non-intervention's application in cyberspace remains unclear, existing principles have some immediate application to cyber operations.

A cyber operation may violate the prohibition on the use of force. The prohibition on the use of force is a fundamental principle of international law, embodied both in the U.N. Charter and in customary international law.[45] The prohibition on the use of force restricts the use of armed force but does not apply to economic or political coercion.[46] Economic and political coercion often violate international law—specifically, the principle of non-intervention—but the conventional and customary prohibition on the use of force only regulates the use of armed force.[47] The prohibition on the use of force does not encompass all cyber operations, though the non-kinetic nature of cyber operations blurs the line between armed force and non-armed coercion.[48] The Tallinn Manual is a publication sponsored by NATO and authored by the International Group of Experts, a group of experts on international law and cyber operations who sought to apply existing principles of international law to cyber operations, and to codify emerging customary rules for the law of

---

[44] TALLINN MANUAL, *supra* note 7.

[45] U.N. Charter art. 2, ¶ 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."); CRAWFORD, *supra* note 14, at 746–47. This principle is recognized as a tenet of customary international law. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Jurisdiction and Admissibility Judgment, 1984 I.C.J. 392, ¶ 71 (Nov. 26).

[46] CRAWFORD, *supra* note 14, at 747. Brazil unsuccessfully proposed expanding the prohibition on use of force to economic force during drafting of the U.N. Charter. SHAW, *supra* note 14, at 1019 n.27.

[47] Derek W. Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1 (1972) (discussing the impact of the Declaration of Friendly Relations on the legality of economic and political coercion). Applying the prohibition on the use of force to economic and political conduct is a source of continuing academic discussion. *See* SHAW, *supra* note 14, at 1019–21. However, in its present form, international law still does not consider economic coercion a use of force. CRAWFORD, *supra* note 14, at 747.

[48] TALLINN MANUAL, *supra* note 7, at 47–48; Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 57–59 (2001).

war and cyber operations.[49] The Tallinn Manual proposes eight criteria for determining when a cyber operation constitutes a use of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality.[50] This analytical framework generally seeks to remedy the dearth of state practice and instructive decisions by drawing parallels between cyber operations and conventional operations.[51]

The Tallinn Manual proposes applying existing principles of international law—those that govern the use of traditional military force—to cyber operations.[52] For example, the Manual's criterion of severity provides a bright-line rule: physical harm (beyond a de minimis level) to persons or property is a use of force.[53] Just as a kinetic attack harming

---

[49] TALLINN MANUAL, *supra* note 7, at 1–6.

[50] *Id.* at 48–51. The Tallinn Manual expands these considerations with sample questions:

> (a) Severity: How many people were killed? How large an area was attacked? How much damage was done within this area?
>
> (b) Immediacy: How soon were the effects of the cyber operation felt? How quickly did its effects abate?
>
> (c) Directness: Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects?
>
> (d) Invasiveness: Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country?
>
> (e) Measurability: How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects?
>
> (f) Military character: Did the military conduct the cyber operation? Were the armed forces the target of the cyber operation?
>
> (g) State involvement: Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred?
>
> (h) Presumptive legality: Has this category of action been generally characterized as a use of force, or characterized as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?

Id. at 51 n.22. The International Group of Experts (the ad-hoc group behind the Tallinn Manual) derived this framework from the ICJ's statements regarding the "scale and effects" of a use of force in the *Nicaragua* case. *Id.* at 47 (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 191, 195 (June 27)).

[51] *See id.* at 47–52. For example, Rule 11 states: "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.

[52] "In great part, [the approach] is intended to identify cyber operations that are analogous to other non-kinetic or kinetic actions that the international community would describe as uses of force." *Id.* at 48.

[53] *Id.*

persons or property is likely a use of force, a cyber operation with the same effect is likely a use of force as well.[54] Accordingly, infrastructure-damaging operations, unless the resulting damage is de minimis, will violate the prohibition on use of force. A cyber operation targeting electrical turbines or a dam, for example, would certainly be a use of force if the operation damaged the turbine through over-acceleration or if the operation caused damaging flooding by opening the floodgates of a dam. The Stuxnet worm, because it physically damaged Iranian uranium centrifuges, was a clear use of force.[55] The International Group of Experts was divided on whether Stuxnet was an armed attack, however, which gives rise to the right of armed self-defense.[56]

When a cyber operation does not cause physical damage to persons or property, the Tallinn framework requires a more nuanced comparison of cyber operations to conventional operations.[57] The narrow definition of the use of force, encompassing only military force (to the exclusion of economic and political coercion), means that most cyber operations that do not cause physical damage will not be considered a use of force. A non-damaging cyber operation must still be analogous to a conventional use of force to fall within the prohibition on the use of force. For example, the Tallinn Manual states that "non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force."[58] Cyber operations interrupting the functions of the economy or government of a State would only constitute uses of force if such attacks caused effects on the core national in-

---

[54] *Id.* In other words, a result that would be a use of force if achieved by a bullet or a bomb is no less a use of force if achieved by malicious computer code.

[55] *Id.* at 45. Some members of the International Group of Experts also considered Stuxnet an armed attack. *Id.* at 58.

[56] *See id.* at 52 (noting the difference between the standards of "use of force" and "armed attack"). The International Group of Experts' focus befits their sponsor (NATO)'s interest in *jus ad bello*. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27) (assessing the United States' claim of collective self-defense by noting the difference between "less grave" uses of force and "most grave" uses of force that constitute an armed attack). This Comment focuses on the existence of internationally wrongful acts, a lower standard than that of armed self-defense. *See id.*

[57] *See* TALLINN MANUAL, *supra* note 7, at 48–51. In light of the Tallinn Manual's emphasis on severity, and the difficulty of determining severity absent physical damage, the criterion of measurability becomes more important. *Id.* at 50.

[58] *Id.* at 46. This type of cyber operation may, however, violate the principle of non-intervention. *See Military and Paramilitary Activities*, 1986 I.C.J. ¶ 202; G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations 121, 122 (Oct. 24, 1970).

terests of a State equivalent to a conventional use of force.[59] In other words, to qualify as a use of force, the cyber operation interrupting economic or political functions would have to be equivalent to occupation by a conventional military force. Such an operation would need to have far-reaching, pervasive, and long-lasting effects equal to the effect of a conventional use of force. Therefore, cyber operations that do not affect infrastructure or target military systems will generally lack the requisite degree of severity, directness, and military character to be analogous to a conventional use of force because of the temporary and reversible character of most cyber operations.[60]

Depending on context, however, cyber operations could rise to the level of a use of force by creating effects equivalent to a conventional use of force. For example, using malware to disable the air-defense network of a State for an extended period of time could meet the criteria of a use of force.[61] The military character of the target, coupled with the gravity of the national interest in air defense, likely creates effects similar to a conventional use of force.[62] Similarly, using an infrastructure-interference operation to disable all rail traffic or air traffic in a country could meet the criteria for a use of force because of the scope of the attack alone; a large-scale disruption of such a core national interest as transportation would likely be a use of force if it lasted a significant period of time.[63] Though analogizing a computer virus to a conventional military strike is challenging due to the difference in mechanisms of action, adapting the existing use-of-force and armed-self-defense legal structure can minimize uncertainty in light of changed circumstances.[64] The Tallinn Manual

---

[59] TALLINN MANUAL, *supra* note 7, at 48–52. The 2007 Estonia attack shows the potential for interference with core government functions of even a DoS attack. Schmitt, *supra* note 10, at 569–70.

[60] TALLINN MANUAL, *supra* note 7, at 48–52. Severity, "the most significant factor in the analysis," touches on "the scope, duration, and intensity" of the attack. *Id.* at 48. The severity inquiry also relies heavily on the cyber operation's effect on "critical national interests." *Id.* Network intrusions and DoS attacks generally will not affect a State's core national interests with sufficient scope, duration, and intensity to approximate the effects of a conventional use of force. *See id. But see* Schmitt, *supra* note 10, at 570.

[61] If not a use of force, this act could be a threatened use of force, discussed *infra*.

[62] Such an attack would meet many of the Tallinn criteria: severity (national defense is a core national interest, and such an operation would cause a long-term, nationwide impairment); military character (targeted towards the military of a State); directness; immediacy; and intrusiveness (presuming that the military networks were encrypted). *See* TALLINN MANUAL, *supra* note 7, at 48–52.

[63] Most of the considerations discussed above would be present in a nationwide transportation disruption. However, the military character would be much more attenuated, and the effects would be further from the core national interest. With both this and the preceding example, note that the disruption would have to be widespread, long-term, and complete. *See id.* at 48.

[64] *See* U.N. Charter art 51.

avoids many of the problems inherent in emerging customary principles by applying existing, recognized legal principles to novel circumstances and contexts.[65]

A narrow category of cyber operations may violate the prohibition on threats of force. The prohibition on threats of force—though clearly established in the United Nations Charter and as custom—is not a well-defined rule of customary international law.[66] Assuming that expressing a willingness to use force without legal justification constitutes a prohibited threat of force,[67] threats to engage in cyber operations will violate the prohibition insofar as the threatened operation would be a use of force if carried out.[68] A more interesting question is when a cyber operation—while not itself a use of force—could express a willingness to use force without legal justification. Generally, the core of a threat is the *expression* of willingness to use force.[69] Thus, whether a cyber operation, standing alone, expresses willingness to use force would be highly dependent on circumstances. For example, a cyber operation disabling air defenses could express a State's willingness to use conventional force (i.e., use of missiles, bombs, and bullets via air operations) against another state.[70] Mere demonstration of the capacity to disable air-defense radar, missile

---

[65] TALLINN MANUAL, *supra* note 7, at 48–52.

[66] U.N. Charter art. 2, ¶ 4. Judge Crawford contrasts the relative clarity of "use of force" with the ambiguity of what sort of "threat" Article 2(4) prohibits. CRAWFORD, *supra* note 14, at 747. Specifically, he notes that threats of force both relate to the right of self-defense and play a valuable role in resolving disputes without actual force. *Id.* For a discussion of the value of threats of force in international relations, see Matthew C. Waxman, *The Power to Threaten War*, 123 YALE L.J. 1626, 1647–53 (2014).

[67] More comprehensive (and less succinct) definitions of the prohibition on threats of force exist. *See, e.g.*, Romana Sadruska, *Threats of Force*, 82 AM. J. INT'L L. 239, 242 (1988) ("In the international arena, a threat of force is a message, explicit or implicit, formulated by a decision maker and directed to the target audience, indicating that force will be used if a rule or demand is not complied with."(footnote omitted)). This formulation is adapted from the ICJ's discussion of the prohibition on threats of force. *See* Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 47–48 (July 8). In that opinion, the court concluded that whether or not "a signalled intention to use force if certain events occur is . . . a threat" depends on whether the threatened use of force, if carried out, would be lawful. *Id.* ¶ 47. The Tallinn Manual adopted this understanding of the definition of "threat of force," with the caveat that a threat need not be coercive (though threats usually are made to achieve an end) to violate Article 2(4) and the customary prohibition. TALLINN MANUAL, *supra* note 7, at 52–53.

[68] TALLINN MANUAL, *supra* note 7, at 52; 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, 901 & n.44 (1999).

[69] Sadruska, *supra* note 67, at 242–44.

[70] This type of operation could be a use of force if sufficiently widespread, long-term, and complete. *See supra* note 61 and accompanying text. However, the following discussion assumes that this operation would not be a use of force.

systems, etc., could express a State's willingness to use conventional force without legal justification.[71] The cyber operation itself, in that example, would show that a State is willing (and able) to use force without opposition. Any accompanying communications of the meaning of such an operation would increase the expressive nature of the operation; however, the circumstances of the operation standing alone could create a threat of force. The hypothetical air-defense disruption would express a clearer threat of force if it focused on a potential target, shared border, or other sensitive area. Though this potential for a cyber operation as a use of force exists, most cyber operations target symbolic targets (e.g., DoS attacks on the website of a State's organ) or confidential data (e.g., geopolitical or economic espionage via network intrusions and malware).[72]

A State cyber operation may also violate the principle of non-intervention. This principle flows from territorial sovereignty and is grounded in customary international law.[73] Stated positively, the principle protects "the right of every sovereign State to conduct its affairs without outside interference."[74] A particular challenge in applying this principle to cyber operations is the relation to territorial sovereignty; in other words, how can territorial sovereignty be harmed in a virtual space?[75] However, despite the non-territorial location of cyber operations, they may constitute unlawful intervention if their effects are sufficiently coer-

---

[71] Positive actions, without any further expressions of a willingness to use force, can create threat. *See* Sadruska, *supra* note 67, at 243.

[72] *See generally* TIKK ET AL., *supra* note 11 (studying four representative cyber-operation DoS attacks, two involving DoS attacks against State organs, and one involving defacement of websites in defiance of a government order).

[73] The *Nicaragua* judgment recognized the principle of non-intervention as custom. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27). The *Nicaragua* court noted approval of the principle in (among other authorities) the *Corfu Channel* judgment, the Friendly Relations Declaration, and the Helsinki Final Act. *Id.* ¶¶ 202–204 (citing Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 34–35 (Apr. 9), G.A. Res. 2625, *supra* note 58, at 121–22, and Final Act of the Conference on Security and Cooperation in Europe, Aug. 1, 1975, 14 I.L.M. 1292); *see also* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 429; SHAW, *supra* note 14, at 191.

[74] M*ilitary and Paramilitary Activities*, 1986 I.C.J. ¶ 202.

[75] In *Nicaragua*, the ICJ delimited the concept of territorial sovereignty to the land, internal waters, territorial sea, and airspace above that territory. *Id.* ¶ 212. Cyber operation scholarship largely focuses on the *jus ad bellum*/use of force analysis in part because "cyberspace is often regarded as a virtual domain over which no State is able to exercise territorial control." Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SECURITY L. 211, 222 (2012). Buchan argues that sovereignty protects the decision-making capacity of the State, not just its borders, airspace, and waters. *Id.* at 222–25. He points to the 2007 Estonia incident as an example of the coercive effect of cyber operations. *Id.* at 225–26; *see also* TIKK ET AL., *supra* note 11, at 21–23 (describing the targets of the 2007 Estonia attack).

cive.[76] This analysis requires distinguishing between permissible foreign policy (economic sanctions, public comments on events in other States) and impermissible interventions (efforts that "depriv[e] the state intervened against of control over the matter in question.")[77] While all cyber operations generally will coerce some outcome, to constitute an unlawful intervention, that outcome must be one that the target State has the sovereign right to control.[78] Though some of these outcomes are clear (e.g., government policy), others are harder to determine whether a State has the sovereign right to control (e.g., the release of a film). Equally challenging in some cases may be determining the desired outcome. For example, in a network intrusion seeking to steal restricted data, is there any coercion?[79] Though the target State may claim that it was coerced into allowing the conveyance of that data against the citizen's wishes (a somewhat inverted form of expropriation, perhaps), that argument likely depends on the data or the citizen's relation to sovereign functions.[80] The

---

[76] The principle of non-intervention, at its core, protects the right of a State to carry on its affairs and choose its policies without external coercion. M*ilitary and Paramilitary Activities*, 1986 I.C.J. ¶ 205.

[77] OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 432. As State practice shows, the customary principle of non-intervention does not bar all actions intended to change the conditions in another State. *Id.* The *Nicaragua* court determined that economic sanctions and related acts were not unlawful interventions. M*ilitary and Paramilitary Activities*, 1986 I.C.J. ¶¶ 241–242. However, the actions violating the principle of non-intervention in that case—funding and training anti-government armed rebels—were "particularly obvious" violations of the principle, which does not help determine the boundary of unlawful interventions. *Id.* ¶¶ 205, 242. Beyond those examples, though, the underlying substantive rights of the principle of non-intervention show the type of coercion the principle protects against:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.

Id. ¶ 205.

[78] *See* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 14, at 432. Applying this rule to the 2007 Estonia dispute, Buchan concludes that the location of a war memorial (the outcome that the cyber operation sought to change) is a decision that a sovereign is entitled to make. *See* Buchan, *supra* note 75, at 226.

[79] Standing alone, economic cyber espionage seems to be "an unfriendly act but not a violation of international law." Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1182–83 (2014) (internal quotation marks omitted). Skinner notes that, as with conventional espionage, States tolerate economic cyber espionage because they wish to engage in it themselves. *Id.* at 1183.

[80] Skinner argues that economic cyber espionage is a violation of the principle of non-intervention by infringing on the State's "proprietary economic space." *Id.* at 1190. Beyond control over the domestic economic sphere, the State likely has a

complex territoriality of cyberspace makes the State's right to exercise control over the digital information and property of its citizens unclear.[81] This may require viewing network intrusions as the outcome itself, rather than a means of coercing an outcome. Under that model, a target State could argue that the network intrusion coerced the State into allowing breaches of privacy and invasions of property rights, which the State has a right to regulate internally. In turn, the intruding State could argue that the target State took no actions, and was therefore coerced to do nothing. Without further development of international law in this area, the answer remains unclear.

However, the law of non-intervention should expand and adapt in response to cyber operations and their effects.[82] In practice, most cyber operations have economic and political targets and effects.[83] The law of non-intervention protects a State's right to choose "a political, economic, social and cultural system."[84] Accordingly, the law of non-intervention should address most cyber operations. Cyber operations present a new problem, though—the internet makes interference with another State's internal affairs much easier. For example, the Sony incident—at least as construed by the United States—allowed North Korea to influence the distribution of a film within the United States.[85] This incident highlights the coercion issue raised in the preceding paragraph and its importance

---

sovereign right to choose to protect the confidentiality of military designs, diplomatic cables, and the identity of intelligence assets. Seeking such information is quintessential espionage, though, and State practice shows that seeking such information is common practice. Its limits depend more on territorial sovereignty than on principles of coercion. *See* Simon Chesterman, *Secret Intelligence*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶¶ 14–15 (2009) (discussing violations of the principle of non-intervention with examples of unauthorized use of territory and violations of sovereign airspace, not by any form of coercion).

[81] For a discussion of the complex territoriality of the internet, see Molly Sauter, *Cyber Warfare: Show Me on the Map Where They Hacked You: Cyberwar and the Geospatial Internet Doctrine*, 47 CASE W. RES. J. INT'L L. 63 (2015). Sauter concludes that a "geographic metaphor" attributing territorial aspects to portions of the internet is conducive to questions of international law but may be harmful to the internet as we know it. *Id.* at 74–77.

[82] Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 173–74 (2005) (concluding that the non-intervention framework is best suited to address cyber operations without physical effects).

[83] *See* Mary Ellen O'Connell, *Cyber Security Without Cyber War*, 17 J. CONFLICT & SECURITY L. 187 (2012) (arguing that the law of war does not address most problematic cyber operations).

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

[85] In fact, Sony's decision not to release the film in response to threats from the "Guardians of Peace," apparently changed President Obama's decision-making as to his response. *See* Sanger et al., *supra* note 3.

in the cyber-operations context.[86] The conventional coercion inquiry looks for foreign intervention's influence on State actions.[87] However, the same State interests may be influenced by targeting private parties instead of the State, as the Sony incident shows.[88] Therefore, the law of non-intervention should expand the coercion inquiry to consider the potential for coercion of the State in cyber operations targeting non-State actors. Where a cyber operation does not coerce action by the State, but has a substantial effect on a core State interest (e.g., political, economic, or social affairs), the law of non-intervention should prohibit such operations. Whether the law currently does or will change to do so remains to be seen.

B. Attribution of Cyber Operations to the State

This Part will briefly explore when State cyber operations are attributable to the State, focusing predominately on the Articles on State Responsibility.[89] While technical attribution is a substantial evidentiary issue, this Part will focus solely on applying the international legal standards of attribution to the cyber context.[90] First, some potential perpetrators of cyber operations would be considered organs of the State under Article 4.[91] The acts of State-owned companies and similar entities are also attributable to the State under Article 5. [92] Finally, private groups op-

---

[86] *See supra* notes 75–81 and accompanying text (discussing the coercion issue that arises from cyber operations, especially those that do not target the State itself).

[87] *See supra* notes 72–74 and accompanying text (describing the conventional coercion inquiry).

[88] *See* Sanger et al., *supra* note 3.

[89] *See supra* note 10; *see also supra* notes 34–35 and accompanying text (discussing the authoritative weight of the work of the International Law Commission). Condorelli & Kress note the "tripartite model" of State responsibility—attribution, breach, and lack of circumstances precluding wrongfulness—as both a "faithful reflection" of modern practice and the model explicitly used by the ICJ. Luigi Condorelli & Claus Kress, *The Rules of Attribution: General Considerations*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 37, at 221, 224.

[90] Technical attribution is a substantial evidentiary hurdle for States seeking to hold other States accountable for cyber operations. Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SECURITY L., 229, 234 (2012) (noting the technical difficulty of both tracing an operation to a particular computer and specific individuals or organizations); *see also* TALLINN MANUAL, *supra* note 7, at 39–40 (recognizing that, even when cyber operations are traceable to governmental cyber infrastructure, such tracing is not sufficient to prove attribution to the State).

[91] TALLINN MANUAL, *supra* note 7, at 30–31.

[92] Articles on State Responsibility, *supra* note 9, at art. 5.

erating at the express direction or control of a State may be de facto organs of the State under Article 8.[93]

First, the actions of the organs of a State are always attributable to the State.[94] Organs of a State include all components of the State's administrative organization.[95] And, as discussed further in Part III.A *infra*, police agencies' failures to enforce internal laws against cyber operations are attributable to the State. This includes *ultra vires* acts of a State organ.[96] Therefore, any cyber operations undertaken by an organ of a State will be attributed to the State, so long as that act is undertaken in official capacity or under color of authority.[97] A real-world example of this is China's People's Liberation Army (PLA) Unit 61398, which is the subject of a detailed report by Mandiant, a multi-national cyber security company.[98] Unit 61398 appears to be a formal part of the Chinese military, which is an organ of the Chinese state.[99] Assuming the accuracy of Mandiant's report, Unit 61398 undertakes its cyber operations in its capacity as an organ of the Chinese State.[100] Without determining whether its various operations violate any of China's obligations under international law, Unit 61398's actions are almost certainly attributable to China. Other States with military cyber-operations units are similarly responsible for the actions of those military units.[101]

Second, the conduct of State-owned companies and other private entities with public responsibilities can be attributable to the State.[102] The

---

[93] *Id.* at art. 8.

[94] *Id.* at art. 4.

[95] JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY 94 (2002).

[96] Articles on State Responsibility, *supra* note 9, at art. 7.

[97] CRAWFORD, *supra* note 95, at 94–95, 99.

[98] MANDIANT, APT1: EXPOSING ONE OF CHINA'S ESPIONAGE UNITS (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (concluding that Unit 61398 is a unit of the Chinese military and responsible for a number of cyber operations); *see also* 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, 276 (2013) (discussing Unit 61398 and its impact).

[99] *See* Articles on State Responsibility, *supra* note 9, at art. 4. The military of a State is an organ of that State, as it carries out a core function of that State. *See* CRAWFORD, *supra* note 95, at 103 (discussing armed forces as an organ of a State).

[100] For example, "China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense." MANDIANT, *supra* note 98, at 3.

[101] The United States' Cyber Command, "a sub-unified combatant command," coordinates the cyber-operation capacities of the Army, Navy, Air Force, and Marine Corps. *U.S. Cyber Command Factsheet*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/2/Cyber_Command/. Its actions and those of its constituent parts are attributable to the United States for the reasons stated in note 99.

[102] Articles on State Responsibility, *supra* note 9, at arts. 5, 8; CRAWFORD, *supra* note 95, at 100–02.

conduct of private entities is attributable to the State when internal law empowers the entity to act on behalf of the State, and the conduct in question is in that quasi-governmental role.[103] Judge James Crawford, a current Judge of the International Court of Justice, former U.N. Special Rapporteur on State Responsibility, and noted international legal scholar, proposes that this inquiry depends on "the particular society, its history and traditions."[104] While this inquiry generally narrows the scope of State responsibility for the conduct of entities other than those that exercise core government functions, the legacy of State-owned private industry in communist States such as China and North Korea raises interesting concerns for industrial espionage.[105] However, despite his relativist test, it appears from Crawford's commentaries that a collectively owned economic system, without more, likely does not transform every State-owned company into an organ of the State.[106] State-owned companies are more likely to have conduct imputed to the State where their area of responsibility relates to national security or defense activities, traditional areas of State responsibility; however, the conduct of sufficiently controlled companies may also be imputable to the State under Article 8.[107] Emerging government-authorized private cyber-response forces[108] might be imputed to their authorizing State if they are seen as exercising part of the governmental power of national defense.[109]

---

[103] CRAWFORD, *supra* note 95, at 100–01.

[104] *Id.* at 101. Judge Crawford frames this inquiry as "essentially . . . the application of a general standard to varied circumstances." *Id.*

[105] Judge Crawford gives privately run prisons and railroad police as examples of this privately exercised governmental authority. *Id.* at 100–01.

[106] *Id.* at 100–02. Judge Crawford uses commercial enterprises as examples to show that the powers conferred must be governmental in nature; as an example, he states that a railway company with limited police powers is not responsible for its actions as a commercial concern, only as a private police force.

[107] *Id.* at 112–13.

[108] For example, the "Enhanced Cybersecurity Services" program allows private companies, including defense contractors and infrastructure managers, access to classified intelligence to enable cyber defense. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (authorizing the program); *see also* Shane McGee, Randy V. Sabett & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. TECH. L. 1, 40–43 (2013) (proposing limited cyber operations in response to attacks from State actors). Though the "active defense" that McGee, Sabett, and Shah propose is responsive (and either exercises the lawful right to self-defense or constitutes a lawful countermeasure), consider an initial cyber operation that does not violate international law followed by a response that does.

[109] Articles on State Responsibility, *supra* note 9, at art. 8.

III. CYBER OPERATIONS PERPETRATED BY NON-STATE ACTORS

As a complement to Part II, this Part will consider when cyber operations by non-State entities and actors may give rise to internationally wrongful acts attributable to a State. Part III.A will assess when the conduct of non-State entities, both companies and "hacker groups" can be attributed to the State due to direction, control, or ratification. Part III.B will discuss State responsibility for cyber operations not attributable to the State. States may violate the prohibition on transboundary harm by allowing known but unattributable cyber operations. States may also be subject to an obligation to enforce internal laws against perpetrators of (domestically) unlawful cyber operations.

A. Attributing Non-State Cyber Operations to the State

In contrast to the relative clarity of attributing the actions of the organs of a State to the State, the State is generally not responsible for the actions of other entities (e.g., citizens of the State).[110] States, as autonomous persons of international law, are only responsible for actions that can be imputed to an action or omission of the State.[111] The International Court of Justice explicitly rejected any kind of strict liability for acts carried out within the territory of a State in the *Corfu Channel* case.[112] Therefore, analysis of State responsibility for the acts of persons and entities within the State turns on "a legal, functional, or factual link" between the wrongful act and the State.[113] This Part will consider three links: a factual link through direction, control, or ratification; a functional/legal link through knowledge of and inaction towards transboundary harm; and a legal link through a failure to enforce internal laws against transnational aggressors.

First, and perhaps most logically, a State is responsible for conduct it directs, controls, or ratifies, as codified under Articles 8 and 11 of the Articles on State Responsibility.[114] Any attribution under Article 8 is a high

---

[110] Olivier de Frouville, *Attribution of Conduct to the State: Private Individuals*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 37, at 257, 261–64 (stating the rule of non-attribution).

[111] *Id.* at 261 ("[T]his condition implies that only acts that can be attached to a State objectively through a legal, functional, or factual link or through an organ can be attributed to that State.").

[112] *See* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9).

[113] De Frouville, *supra* note 110, at 261.

[114] Articles on State Responsibility, *supra* note 9, at arts. 8, 11; *accord* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27); De Frouville, *supra* note 110, at 265–75. The Articles on State Responsibility state direction, instructions, and control disjunctively, showing that the International Law Commission intended them to be separate standards. Articles on State Responsibility, *supra* note 9, at art. 8 ("The conduct of a person or group of

standard, as shown in the *Nicaragua* judgment, requiring factual proof of the link between the State and non-State actor.[115] Attribution due to the State's direction or instructions requires a factual link between the State's instructions and the wrongful conduct, meaning an *ultra vires* act cannot be attributed to the State.[116] This requires some evidence of instructions to commit an internationally wrongful act, which a State has a strong interest in suppressing. Effective control, in contrast, denotes continuous and pervasive supervision by and dependence on the State, rather than a specific factual link between instructions and conduct.[117] Therefore, a group under effective control could commit a wrongful act without direction and still create responsibility for the State.[118] Returning to the foundational principle that a State is responsible for its own conduct, this inquiry essentially is whether the actions of the non-State actor are so integrated with the State's wishes that the State is responsible for something it did not do. Where the State instructs a group to engage in specific conduct, the State is responsible for that conduct. Where the State closely controls a group, the State is responsible for all of the group's conduct—essentially, as a de facto organ of the State.[119] Finally—and

---

persons shall be considered an act of a State under international law if the person or group of persons is in fact acting *on the instructions of, or under the direction or control of,* that State in carrying out the conduct." (emphasis added)).

[115] *Military and Paramilitary Activities*, 1986 I.C.J. ¶ 115. The United States' funding, training, and supply of the Contras was insufficient to demonstrate the effective control required to establish responsibility for their acts. Similarly, no evidence showed that the United States directed the Contras to carry out any of the acts in question. *See also* CRAWFORD, *supra* note 95, at 110 (emphasizing the requirement of a factual link).

[116] CRAWFORD, *supra* note 95, at 110 n.160, 154 (noting that direction and control have important semantic differences in languages other than English); De Frouville, *supra* note 110, at 268–69. The difference between acting on instructions or under direction appears minimal: both require a factual instructions-to-conduct link. De Frouville, *supra* note 110, at 270. De Frouville is skeptical of any differentiation between the three conditions. *Id.* at 271 ("The only notable difference is in fact temporal: in one case a factual link at a particular point, while in the other, 'control' constitutes a continuous factual link."). However, the ability to infer instructions that a State has a strong incentive not to give directly—i.e., orders to commit an unlawful act—seems useful in practice.

[117] CRAWFORD, *supra* note 95, at 110–13; De Frouville, *supra* note 110, at 269–71.

[118] CRAWFORD, *supra* note 95, at 113. However, note that the requisite control is a very rigorous standard. *See Military and Paramilitary Activities*, 1986 I.C.J. ¶¶ 113–115. *But see* Prosecutor v. Tadic, Case No. IT-94-1-I, Judgment, 38 I.L.M. 1518, ¶¶ 116–17 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (stating that effective control should be a variable standard according to the circumstances, and criticizing the ICJ ruling in *Nicaragua*). De Frouville notes the oddity of a criminal court delving into the law of state responsibility, but describes the Appeals Chamber's approach as "useful." De Frouville, *supra* note 110, at 270.

[119] De Frouville, *supra* note 110, at 268, 271.

briefly—a State may adopt the conduct of a non-State actor as its own by ratifying that conduct.[120]

Before applying this doctrine to cyber operations, explanation of the phenomena of "patriotic hackers" may be helpful. Hackers and hacker groups are a common phenomenon—persons skilled in cyber operations, with widely varying degrees of organization, who engage in cyber operations (here, the term is used for the sake of consistency rather than particular descriptiveness, as operations may imply greater organization than is generally present), either for monetary gain, political/ideological purposes, or for general amusement.[121] A subset of these groups are patriotic hacker groups, who engage in similar behaviors as other hacker groups, but to achieve political objectives, either on behalf of the State's perceived interest or to avenge a perceived slight to the State.[122] At least nominally, a (presumably North Korean) hacker group calling itself "Guardians of Peace" was behind the 2014 Sony attack.[123] The 2007 Estonia attacks show the breadth of patriotic hacking. The attacks seem to have been perpetrated in part by a distributed mass of Russian activists—some members of the Russian pro-government youth group "Nashi"—

---

[120] Articles on State Responsibility, *supra* note 9, at art. 11; De Frouville, *supra* note 110, at 273–75. Ratification requires not just approval, but endorsement of the wrongful conduct. De Frouville, *supra* note 110, at 274 (citing United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶¶ 58, 74 (May 24) (holding that Iran had no responsibility for the hostage-takers' conduct until it ratified and encouraged the hostage crisis—which made the hostage-takers effectively agents of the State)).

[121] A common term for politically motivated hackers is "hacktivists." *See, e.g.*, Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 546 (2012). Perhaps the best-known hacker group is Anonymous, an amorphous but influential collective responsible for a number of cyber operations. *See* David Kushner, *The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson*, NEW YORKER, Sept. 8, 2014, at 48, 53. Illustrative of the low end of the organization spectrum, Kushner states:

> It was a new kind of hacker collective. 'It's not a group,' Mikko Hypponen, a leading computer-security researcher, told me—rather, it could be thought of as a shape-shifting subculture. Barrett Brown, a Texas journalist and a well-known champion of Anonymous, has described it as "a series of relationships." There was no membership fee or initiation. Anyone who wanted to be a part of Anonymous—an Anon—could simply claim allegiance.

Id. at 50.

[122] TIKK ET AL., *supra* note 11, at 31–32; *see also* Gervais, *supra* note 121, at 546.

[123] Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

using instructions posted online.[124] However, as discussed below, their conduct likely cannot be attributed to Russia.

Due to the confluence of the State's interests and the patriotic hacker groups' targets and objectives—as well as plentiful allegations that patriotic hacker groups act either in concert with or at the whim of the State—questions of State responsibility arise.[125] Applying the Article 8 direction or control test to Nashi's involvement in the 2007 Estonia cyber operations, the analysis begins with the group's factual relationship to the State.[126] Tikk, Kaska, and Vihul—in their thorough analysis of the 2007 Estonia attacks—do not assert that the Kremlin or any organ of the State ordered the operations.[127] Therefore, it is necessary to consider "effective control" under Article 8. Nashi is a pro-government group, created and funded by the Kremlin, with no small measure of ideological control over the group.[128] However, it appears to be supported by the State more than controlled by it.[129] As a group funded and supported by the State, but not pervasively directed and guided by the State, Nashi seems substantially similar to the contras in Nicaragua—and, under that standard for control, its conduct is not attributable to the State.[130] This example illustrates the difficulty of establishing control over hacker groups. Most groups, even those with substantial and deep connections to the State, are not so pervasively dependent and controlled to meet the effective-control standard.

B. Separate International Obligations Created by Non-State Cyber Operations

Since cyber operations by non-State actors likely will not be attributable to the State, when does the State's response to an unlawful cyber

---

[124] TIKK ET AL., *supra* note 11, at 23 (describing the initial attackers as substantially comprised of "crowds affected by nationalistic/political emotions who carried out the attacks according to the instructions provided in Internet forums and websites").

[125] Gervais, *supra* note 121, at 546–47.

[126] *See supra* notes 114–119 and accompanying text.

[127] TIKK ET AL., *supra* note 11, at 23–24.

[128] Nashi has considerable ideological, leadership, and financial links to the Kremlin, and was created by the Kremlin to counter the potential for an anti-government youth movement in Russia. Steven Lee Myers, *Youth Groups Created by Kremlin Serve Putin's Cause*, N.Y. TIMES (July 8, 2007), http://nyti.ms/23TacL.

[129] *Id.* The group certainly serves the State's purposes, and would likely act on its instructions, but does not appear to act entirely at the whim of the State. The founder of Nashi reportedly stated that "[i]t is very important not to take too strict or rigid control of these movements" to avoid the mistakes of the Komsomol, the youth wing of the Communist Party of the Soviet Union. *Id.*

[130] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 110 (June 27). The contras were "largely financed, trained, equipped, armed and organized" by the United States, and generally served American foreign-policy interests in Nicaragua. *Id.* ¶¶ 95, 108. However, the ICJ found that even "crucial" state support does not establish complete control. *Id.* ¶ 110.

operation violate its obligations under international law? To answer that question, this Section will next apply the customary prohibition against transboundary harm (whether caused by the State or by private actors) that is known of and tolerated by another State, as laid out in the *Corfu Channel*[131] and *Trail Smelter*[132] decisions.[133] The prohibition on transboundary harm obligates a State not to knowingly allow its territory to be used contrary to the rights of another State.[134] This principle, as put forth in the *Corfu Channel* case, begins with the customary principle "that a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation."[135] If the State knew, or reasonably should have known, that the act was occurring, the State is responsible for the act notwithstanding its lack of complicity in the act.[136] In *Corfu Channel*, the court found that Albania reasonably should have known that the Corfu Channel was mined because the Albanian government kept a close watch on the Channel.[137] This knowledge, and Albania's inaction as to the mines, created responsibility to the United Kingdom for the mines' effect, even though Albania did not lay the mines.[138] By analogy, a cyber operation originating within a State could create responsibility for that State if the requisite knowledge or constructive knowledge existed.[139] Just as Albania kept a close eye on the Corfu Channel, at least one major source of cyber operations keeps a very close eye on its internet traffic—China.[140] Moreover, scholars pro-

---

[131] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9).

[132] Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (1941).

[133] This principle is commonly applied to unattributable cyber operations. *See, e.g.*, Schmitt, *supra* note 10, at 602–03; Skinner, *supra* note 79, at 1190–91; Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SECURITY L., 229, 242 (2012).

[134] *Corfu Channel*, 1949 I.C.J. at 18, 22 (holding that a State is only responsible for wrongful acts committed using its territory when the State knew or reasonably should have known of those acts and failed to take action to stop them).

[135] *Id.* at 18.

[136] *Id.*

[137] *Id.* at 18–22.

[138] *Id.* at 22. The mines were actually laid by Yugoslavia. CRAWFORD, *supra* note 14, at 543.

[139] The applicability of principles of territorial control to cyber operations is not a foregone conclusion. *Compare* Buchan, *supra* note 75, at 222 (asserting that States cannot exercise territorial control over cyberspace), *with* Lotrionte, *supra* note 6, at 890–91 (applying principles of territorial control in analyzing self-defense against non-State perpetrators of cyber operations within the territory of a non-cooperative State). Perhaps these views can be reconciled—cyberspace itself is extraterritorial, while the perpetrators of cyber operations exist in physical (territorially controlled) space. However, the operations themselves exist in a metaphysical grey area: they emanate from a specific State, have effects in a specific State, but exist and travel in an extraterritorial virtual space.

[140] *See Corfu Channel*, 1949 I.C.J. at 18; Messerschmidt, *supra* note 98, at 308–309.

pose a cyber-specific obligation of due diligence to monitor outgoing internet traffic for hostile transnational cyber operations.[141] But this obligation remains an emerging customary principle, not yet binding on States.[142]

However, even States without robust internet monitoring could incur responsibility for transboundary harm once ongoing cyber operations within the State reach a level at which the State knows or reasonably should know that cyber operations are ongoing.[143] Existing principles of international law do not sufficiently address a State's obligations in the face of an ongoing, unattributed cyber operation. For example, in the 2007 Estonia attacks, the Russian government likely had enough information to know that the ongoing cyber operations were based—at least in part—inside Russian territory.[144] The perpetrators of the attack were not widely not known during the attacks, though.[145] Despite that fact that Russia's post-incident legal response was less than ideal, its obligations to prevent ongoing transboundary harm were not well defined.[146]

Suppose, then, that a State knows that a cyber operation is ongoing in its territory, but does not know the identity of the perpetrators or have China's internet monitoring/censorship capacity. What are that State's obligations? The language of *Corfu Channel* suggests that the obligation is to prevent using the State's territory to harm another State, and thus that any resulting harm is the responsibility of the State.[147] This formulation suggests absolute liability (i.e., Albania's obligation was to prevent, not to try to prevent). But, in *Corfu Channel*, Albania took no action, despite a clear action being available (warning the British ships about the mine-

---

[141] *See, e.g.*, Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 7, at 189, 208; *see also* Budapest Convention on Cybercrime arts. 20–21, Nov. 23, 2001, 2296 U.N.T.S. 167 (requiring monitoring of traffic and content data).

[142] Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 151 (2013) (noting that the existence of a duty to monitor is "far from settled" and likely conflicts with ideals of free communications).

[143] *See Corfu Channel*, 1949 I.C.J. at 22 ("[T]he laying of the minefield which caused the explosions on October 22nd, 1946, could not have been accomplished without the knowledge of the Albanian Government.").

[144] The attacks continued and escalated from April 30 until May 18. TIKK ET AL., *supra* note 11, at 18–20. During that time, the Nashi group—an organization with close ties to the governing United Russia party and highly placed officials in the government—was involved in some of the cyber operations. Instructions on attacks and targets were also posted on Russian-language websites. *Id.* at 23–24.

[145] *Id.*

[146] An interesting aspect noted in TIKK ET AL. is Russia's refusal to engage in post-incident criminal cooperation, despite a 1993 bilateral treaty promising such cooperation. *Id.* at 27. This was likely a political rather than legal consideration on the Russian government's part. *Id.* at 27–28.

[147] *See Corfu Channel*, 1949 I.C.J. at 22.

field).[148] Where no such option is available, due diligence in attempting to cease the cyber operations may be sufficient.[149]

IV. PRIVATE COUNTERATTACKS AFTER STATE CYBER OPERATIONS

To conclude this Comment, this Part will consider the potential aftermath of State cyber operations against private entities—such as the 2014 Sony incident.[150] Though that incident ended in an apparent State counter-operation by the United States, it could easily have ended in a private counter-operation by Sony against North Korea. Such a counter-operation would have ramifications under international law, even when not conducted by the State. First, two relevant legal justifications could apply to counter-operations: the countermeasures doctrine and the right to self-defense. However, the propriety of State-sanctioned private counter-operations is dubious—granting legal authority to private actors to carry out retaliatory cyber operations likely creates substantial State responsibility for the conduct of private parties. In discussing these possibilities, assume that both the initial cyber operation and the counter-operation constitute breaches of international obligations.

First, it is important to note that a private counter-operation—standing alone—is not attributable to the State nor does it otherwise create State responsibility in the same ways as an offensive cyber operation.[151] Therefore, four possibilities exist as to the lawfulness of the initial cyber operation and the counter-operation. Those permutations are shown below and numbered for reference:

---

[148] "In fact, Albania neither notified the existence of the minefield, nor warned the British warships of the danger they were approaching." *Id.* However, under the Court's wording that "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States," the effect of such a warning on any damage done by the mines is unclear. *See id.*

[149] Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, Report of the Int'l. L. Comm'n., U.N. GAOR, 53rd Sess., U.N. Doc. A/56/10, art. 3(8) (2001); Messerschmidt, *supra* note 98, at 304–05. For a discussion of applicable principles written long before cyber operations were a possibility, see MANUEL R. GARCÍA-MORA, INTERNATIONAL RESPONSIBILITY FOR HOSTILE ACTS OF PRIVATE PERSONS AGAINST FOREIGN STATES 49–66 (1962). García-Mora argued that State practice shows *opinio juris* of an obligation to "refuse the use of its territory and resources for the organization of military expeditions against states with which [a State] is at peace." *Id.* at 49. He notes that the required measures of prevention are uncertain, and that "whether a state is to prevent the formation of a hostile expedition is inevitably limited by the capacity of the state, which must be interpreted as being as far as possibilities will reasonably permit." *Id.* at 63. This suggests that a good-faith attempt to halt a cyber operation would meet a State's international obligation.

[150] *See supra* notes 1–3 and accompanying text.

[151] *See supra* Part III.

Table 1: Possible combinations of lawful and unlawful initial and counter-operations

	Lawful counter-operation	Unlawful counter-operation
Lawful initial operation	1: No wrongful act	2: Only responding State commits a wrongful act
Unlawful initial operation	3: Only initiating State commits a wrongful act	4: Both States commit wrongful acts

In Scenario 1, both States acted within their rights. This would occur if both the initiating and responsive States' actions did not breach any obligations, possibly due to the nature of the operation (e.g., espionage) or the lack of involvement (e.g., a private cyber operation originated from within the State). This scenario does not make for a particularly interesting discussion. In Scenarios 2 and 3, the breach is unilateral. Scenario 2 could arise if the initiating State did not commit a wrongful act, but the counter-operation breached an obligation in its response. (For example, a lawful network intrusion is countered with an infrastructure-damaging operation.) Scenario 3 is likely to arise if a State launches an unlawful cyber operation, and the responding State's counter-operation falls within the doctrine of countermeasures or self-defense. Finally, in Scenario 4, both the initial operation and counter-operation breach the obligations of the respective States. This Part will focus on Scenarios 2 and 3 in exploring the possibilities of private counter-operations.

Preliminary to a discussion of either Scenario, an overview of countermeasures and self-defense is necessary. Condorelli and Kress, in discussing State responsibility, add a third branch to the traditional breach/attribution analysis: the "absence of any circumstance precluding wrongfulness."[152] A counter-operation, then, will be consistent with the legal rights and responsibilities of a State so long as it is justified by either doctrine or another circumstance precluding wrongfulness.[153] The doctrine of countermeasures allows States to suspend observation of an international obligation (and to take action accordingly) to compel another State to cease its wrongful conduct or make reparations for that conduct.[154] Self-defense refers to the right of a State to respond to an armed attack with force, so long as the response is necessary, immediate,

[152] Condorelli & Kress, *supra* note 89, at 224.

[153] *Id.*; Articles on State Responsibility, *supra* note 9, at arts. 21–22 (self-defense and countermeasures), 20, 23–26 (detailing other circumstances precluding wrongfulness such as consent and necessity); Stephen Moore, Comment, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C. J. INT'L L. & COM. REG. 223, 246–49 (2013) (describing the role of both doctrines in responding to a cyber operation and the need for a convention clarifying the law applicable to these doctrines in cyberspace).

[154] Articles on State Responsibility, *supra* note 9, at arts. 22, 49–53.

and proportionate.[155] Self-defense is limited to circumstances where wrongful conduct is ongoing or reasonably likely to resume.[156]

Scenario 2 is useful to illustrate the critical risk inherent in counter-operations. Often, counter-operations will occur in the midst or immediate aftermath of a cyber operation.[157] The wrongfulness or attribution of the initial operation may not be clear to the targeted State.[158] In attempting to respond to a cyber operation and prevent future damage, the targeted State could launch a counter-operation either exceeding the scope of allowable retaliation or against the wrong entity. For example, a State could mistake an incident of "patriotic hacking" for a State cyber operation, and carry out a cyber operation against the government or military of the State without legal justification. Or, a State could respond to an incident of cyber espionage with an infrastructure-damaging attack that amounts to an unlawful intervention or a use of force (which would likely exceed the scope of permissible countermeasures even if the initial act created State responsibility). As discussed in depth below, the risks of a counter-operation during or shortly after an incident are substantial.

Scenario 3 reflects the best-case scenario for a responding State: that it correctly determines that the precipitating effect is a wrongful act attributable to the State and that its response is within the scope of permitted retaliation. If the precipitating act is equivalent to an armed attack,

---

[155] TALLINN MANUAL, *supra* note 7, at 59–66 (codifying imminence of the threat and immediacy of the response as temporal elements of this analysis); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 194 (June 27). Whether or not an armed attack by a non-State aggressor allows self-defense is an open question. The I.C.J. has concluded that Article 51 of the U.N. Charter does not authorize self-defense against non-State aggressors. Legal Consequences of Construction of Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9). This decision stands in stark contrast to the emerging customary law surrounding counter-terrorism and self-defense. Lotrionte, *supra* note 6, at 889 (discussing recent international recognition of the right to self-defense against terrorist organizations). This is not a new idea, however. GARCÍA-MORA, *supra* note 149, at 115–16 (discussing the *Caroline Affair*, in which the U.K. claimed the right to destroy an American pirate ship when the United States was unwilling or unable to prevent acts of piracy).

[156] Lotrionte, *supra* note 6, at 890–91. The ICJ took a restrictive view of self-defense against likely-to-recur armed attacks, stating that a complaint should precede armed self-defense when the attack was not currently ongoing. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶¶ 140–153 (Nov. 6) (holding that an attack on military forces stationed on an oil platform did not show necessity without a prior complaint about attack from the platform).

[157] Indeed, determining the source of a cyber operation with the degree of certainty that the legal system expects may be impossible in many cases. McGee et al., *supra* note 108, at 31, 35–36.

[158] For example, the perpetrators of the most coordinated and sophisticated elements of the 2007 Estonia attacks remained largely unknown in 2007. TIKK ET AL., *supra* note 11, at 23.

then the Article 51 right to self-defense protects a necessary and proportional forceful response.[159] Otherwise, some form of counter-operation might be appropriate to compel observance of another State's obligations, such as the prohibition of transboundary harm or the principle of non-intervention.[160] For example, a network intrusion to delete the code used for an infrastructure-damaging operation could be a proportional and necessary exercise of the right to self-defense.[161] Similarly, a reversible malware attack on the command and control entity launching a DDoS attack could be a lawful countermeasure for that attack.[162]

The above examples show the risks of any counter-operation. While the precipitating attack could be unlawful and attributable, and the response proportional and otherwise lawful (Scenario 3), one or both of those conditions could be lacking (Scenarios 2 or 4), and that defect could only become apparent after the fact. Accordingly, States should exercise caution in engaging in counter-operations, especially against other States. Targets should be proportional and related to the precipitating operation.[163] Particularly, States should use the same caution in using forceful cyber weapons as they do in using kinetic weapons, and for the same reasons.[164] Lesser operations may require lesser caution. In any event, the risks of a counter-operation are substantial, especially when the effects and impact of a cyber operation remain unclear.

These risks guide consideration of private counter-operations. Some private actors engage in private counter-operations already ("hack-backs").[165] These counter-operations have similar considerations to offen-

---

[159] *See* TALLINN MANUAL, *supra* note 7, at 59; Moore, *supra* note 153, at 246–47 (stating that self-defense in cyber operations must be proportional).

[160] *See supra* notes 131–146 (discussing transboundary harm in a cyber context), 73–81 (discussing non-intervention in a cyber context).

[161] Manny Halberstam, Note, *Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks*, 46 GEO. WASH. INT'L L. REV. 199, 204–05 (2013).

[162] *See* Messerschmidt, *supra* note 98, at 318–23. Reversibility is important under Article 49. *See* Articles on State Responsibility, *supra* note 9, at art. 49 cmt. 9. The lack of permanent harm that makes the effect of a cyber operation so nebulous, though, makes compliance with Article 49 much simpler. A permanent cyber operation—outside of an infrastructure-damaging operation—is rare.

[163] Messerschmidt, *supra* note 98, at 318–23.

[164] *See* TALLINN MANUAL, *supra* note 7, at 59–63.

[165] Messerschmidt, *supra* note 98, at 276–77. Google is a well-publicized example of this:

> On January 12, 2010, Google, Inc. publicly announced that another group, now identified as the Elderwood Gang, had infiltrated the company's network along with at least thirty other U.S. companies. The attack, nicknamed "Operation Aurora," was traced to servers at two Chinese educational institutions. But Google didn't stop at tracing the source of the attack. Launching a "secret counteroffensive," the company gained access to the source of the attack and obtained evidence that suggested possible Chinese government involvement. Matt Buchanan of the tech blog Gizmodo crowed, "it's

sive cyber operations, with the exception that attribution to the State through the State's response to the operation may be mitigated by the responsive nature of the operation.[166] However, the United States and other States have taken increasing steps towards either public–private collaboration on cyber defense or wholesale delegation of cyber defense to the private sector.[167] Both of these permutations of State involvement in private cyber operations raise differing levels of risk to the State.

First, a public–private partnership, involving intelligence-sharing and technological cooperation, would be attributable to the State under Article 8.[168] A State would be responsible for actors that it exercises effective control over, as well as any acts it directs or instructs private actors to carry out.[169] A State would likely be seen as directing a counter-operation if it gives an actor (that it knows to be capable of cyber operations) attribution information such that the aggressor can be targeted.[170] However, delegation of cyber defense to private actors raises a more serious concern under Article 5.[171] Insofar as cyber defense is part of national defense, a private entity empowered to retaliate against cyber aggressors is being entrusted with an element of State power, and thus made a de facto organ of the State.[172] This means that any cyber operations that the private entity carries out will be attributable to the State. The State may have no control over the acts, but will have responsibility as though it carried the acts out.[173] Engaging in limited intelligence and technology sharing subjects States to less legal risk than explicitly delegating cyber defense to private actors and allows the State to choose the cyber operations

---

pretty awesome: If you hack Google, they will hack your ass right back.

Id. (footnotes omitted). Messerchmidt goes on to note that a substantial number of private companies both engage in retaliatory cyber operations and think that the capacity to do so is desirable. *Id.* at 277.

[166] *See supra* Part III.

[167] McGee et al., *supra* note 108, at 4 (describing the Defense Industrial Base pilot project).

[168] Articles on State Responsibility, *supra* note 9, at art. 8.

[169] *Id.*

[170] Targeting information seems more likely to create responsibility than tactical and technical guidance. *Cf.* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 112–16 (June 27).

[171] Articles on State Responsibility, *supra* note 9, arts. 5, 8; Messerschmidt, *supra* note 98, at 322–23 (discussing the risks of allowing private firms to engage in cyber defense on behalf of the State, including targeting errors and disproportionate responses).

[172] Djamchid Momtaz, *Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY, *supra* note 37, at 237, 244–46.

[173] Messerschmidt, *supra* note 98, at 322–23 (discussing the possibility that an otherwise justified counter-operation could be disproportionate or could target an innocent entity).

to which it wishes to be attached. Only States without government cyber capacities should consider legal delegation of cyber defense to uncontrolled private actors because such delegation carries much risk and little reward.

V. CONCLUSION

The Sony incident, as a case study, highlights the challenges of applying existing international law to cyber incidents. Even now, both existence of breach of an international obligation and attribution to North Korea are unclear. However, the American response shows that the United States saw this particular cyber operation as a serious threat.[174] While the Sony incident is now only part of the tapestry of United States–North Korean relations, the counter-operation easily could have escalated into kinetic conflict.[175]

Phillip C. Jessup described sovereignty as "the quicksand on which the foundations of traditional international law are built."[176] The territorial basis of sovereignty is rendered even less stable than Judge Jessup saw it when considering the extraterritorial element of cyberspace. Though many principles of international law can be adapted and applied to cyberspace and cyber operations, the contours and particular challenges of cyber operations present novel and unclear questions of legal rights and responsibilities. From a lawyer's perspective, States should tread lightly and carefully. While the challenges of government, business, and progress demand application, cyberspace remains a murky corner of the already-murky realm of international law.

---

[174] The Sony counter-operation was among the more aggressive responses taken by the United States in response to a cyber operation. An unnamed administration official indicated that the response may have been prompted by Sony's decision not to release *The Interview*. *See* Sanger et. al., *supra* note 3.

[175] The United States announced additional sanctions on North Korea in January, 2015, which the DPRK strongly opposed. *See* Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015); Haroon Siddique, *North Korea Responds with Fury to US Sanctions over Sony Pictures Hack*, GUARDIAN (Jan. 5, 2015), http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony.

[176] PHILIP C. JESSUP, A MODERN LAW OF NATIONS 40 (1948).