International Law and Cyber Technology:
Is it time for a new legal paradigm?

Kenneth Brown, Ph.D.
Halcyon Institute

10 May 2023

Abstract

This report critically examines the widely accepted contention that extant international law applies to cyberspace. Specially, it evaluates how current interpretations of the principles on the use of force and nonintervention apply to the domain and whether this reflects state behaviors. By analyzing the provisions in light of three major cyber events – Estonia (2007), Stuxnet (2009-2010), and the 2016 US presidential election – the article finds that the law contains serious gaps and is inconsistent with state practice. Thus, despite scholars' claims to the contrary, a legal vacuum exists. To address this lacuna, this report argues that the US and likeminded nations, supported by scholarly research, should engage in a purposeful effort to develop a new legal paradigm that is tailored to the domain and consistent with state practice. By looking to other historical efforts, such as those focused on international law relating to the sea, civil air transportation, and terrorism, the article draws important lessons on how best to build a new paradigm that, over time, would greatly improve the legal framework.

Introduction

In June 2017 Maersk, the world's largest container shipping company, was brought to a near standstill when a malware named NotPetya went on a rampage in the organization's computer network.[1] Over the course of three days, NotPetya infected over forty-five thousand personal computers and 150 servers, in the process deleting critical data including manifests, orders, personnel records, and gate access codes. As a direct result, shipping came to an abrupt halt in seventeen ports across the globe and normal operations were interrupted for months. In total, the shutdown cost the company an estimated three hundred million dollars.[2]

The impact, however, was not limited to Maersk, as many other companies, including Merck, FedEx, and Mondelez International, were impacted, with a total estimated cost ranging from one to ten billion dollars.[3] While these figures represent tremendous losses, they do not fully account for the downstream effects of shutdowns across multiple industries and nations, or less quantifiable impacts, such as wasted employee time, missed opportunities, lost prestige, and psychological wear.

Although the source of the malware was initially uncertain, over time state intelligence organizations and commercial security firms determined that it was launched by Russia as part of

---

[1] A Greenberg, 'The Untold Story of Notpetya, the Most Devastating Cyberattack in History' *Wired* (22 August 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world> accessed 3 March 2019.

[2] R Milne, 'Moller-Maersk puts cost of cyber attack at up to $300m' *Financial Times* (16 August 2017) <www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff> accessed 23 January 2019.

[3] R Tehrani, *NotPetya: World's First $10 Billion Malware* (Apex Technology Services 2017) <www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm> accessed 16 January 2019; P Pernik, *Responding to 'the Most Destructive and Costly Cyberattack in History*' (Intl Ctr for Def & Sec 23 February 2018) <icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/> accessed 24 January 2019.

its sustained campaign to undermine Ukraine's government and develop its cyber weaponry.[4] Collectively, this campaign has had dramatic effects in Ukraine, and often elsewhere, as Russia has used cyber technology to cut electrical power, interrupt air and train services, disrupt banking, sever communications, and undermine electoral processes.[5]

Despite the widespread damage these cyberattacks are causing, however, it is unclear whether they contravene international law. Rather, due to cyber technology's relative novelty and rapid evolution, combined with the law's reactive nature and slow development, there is a dearth of legal guidance on how activities in cyberspace should be characterized.[6] As such, it is debatable whether Russia's cyberattacks qualify as a use of force under jus ad bello, violate jus in bello, or breach the principle of nonintervention.[7] This uncertainty leaves states in a difficult position as they lack a solid framework to guide decision-making or calculate consequences for acting in cyberspace. Moreover, the lacuna only encourages bad behavior, undermines the ability

[4] The White House, 'Statement from the Press Secretary' (15 February 2018) <www.whitehouse.gov/briefings-statements/statement-press-secretary-25/> accessed 29 June 2020; UK Foreign Office, 'Foreign Office Minister condemns Russia for NotPetya attacks' (2018) <www.gov.uk> accessed 14 January 2019; T Fox-Brewster, 'Petya or NotPetya: Why The Latest Ransomware is Deadlier than WannaCry' *Forbes* (27 June 2017) <www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/> accessed 15 March 2019; S Michael Kerner, 'Why Ransomware Is Still An Active Threat' *EWeek* (4 March 2019) <www.eweek.com/security/why-ransomware-is-still-an-active-threat> accessed 27 May 2020.

[5] UK Nat'l Cyber Security Ctr, *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (3 October 2018) <www.ncsc.gov.uk/> accessed 14 January 2019; A Matwyshyn, 'Cyber Harder' 24 *J Sci & Tech L* 450 (2018); Greenberg (n 1).

[6] Y Eneyew Ayalew, 'Cyber Warfare: A New Hullaballoo under International Humanitarian Law' (2015) 6 *Beijing L Rev* 209.

[7] M N Schmitt & J Biller, 'The NotPetya Cyber Operation as a Case Study of International Law' *EJIL: Talk!* (11 July 2017) <www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law> accessed 22 February 2019.

of states to respond individually or collectively, and lessens predictability and stability in the international system.[8]

While legal scholars have attempted to fill this gap by applying current international law to cyberspace, their arguments are often convoluted, of limited utility, and inconsistent with state practice.[9] In this article therefore, I will argue that, rather than engaging in the often tortured analyses required to apply extant international law, scholars and foreign policy executives should instead focus on developing a new legal paradigm that accounts for cyber technology's unique characteristics, provides a relevant framework, and accurately reflects state behavior.

To analyze this argument, I will use a qualitative case study approach to assess some of the legal and practical aspects of state cyber activities and how they implicate the existing legal paradigm. This process will involve four steps. First, I will review the extant literature to highlight scholars' main arguments and identify gaps. Second, focusing on the principles relating to the use of force and nonintervention in other states' affairs, I will outline the current legal framework. Third, as evidence of cyber activities and associated state behaviors, I will analyze three incidents: Estonia (2007); Stuxnet (2009-2010); and the US presidential election (2016). As part of this analysis, I will highlight the gaps between state behaviors and the current paradigm

---

[8] M Hathaway, *CIGI Papers No. 127: Getting beyond Norms When Violating the Agreement Becomes Customary Practice* (Ctr for Intl Governance Innovation 2017). <www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf > accessed 21 February 2019); C Lam, 'A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election' (2018) 59 *BCL Rev* 2167; Pernik (n 3).

[9] eg, M Schmitt, 'The Law of Cyber Targeting' 68 *Naval War Coll Rev* 10 (2015); UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 <www.un.org/ga/search/view_doc.asp?symbol=A/70/174> accessed 15 February 2019.

and identify associated challenges. Finally, I will provide a recommended approach for developing the requisite new norms. To support this analysis and discern a feasible way ahead, I will draw upon lessons learned from state efforts to develop international law relating to transnational terrorism, the sea, and international air travel.

Through this process, I will show that attempting to stretch the current international legal framework to fit state actions in cyberspace is counterproductive and that a better approach exists. Although an alternative effort would face its own challenges and would likely fall short in its own ways, considering how critical the technology has become, and how the existing legal framework has routinely failed to constrain malign state behaviors, a uniquely designed paradigm is both logical and necessary.[10]

Literature Review

Within the literature on the applicability of international law in cyberspace there are two primary schools of thought. The first, which reflects the majority view, posits that, while the extant legal framework is inadequate, it plays an important role by filling a would-be vacuum.[11] Much of these scholars' efforts, therefore, focus on interpreting the current law in the context of modern challenges posed by state behaviors and cyber technology.[12]

[10] E Tikk, 'Will Cyber Consequences Deepen Disagreement On International Law?' (2018) 32 *Temp Intl & Comp L J* 185.
[11] T Check, 'Analyzing the effectiveness of the Tallinn Manual's jus ad bellum doctrine on cyberconflict, a NATO-centric approach. Review of the Tallinn Manual on International Law Applicable to Cyber Warfare. By Michael Schmitt, ed' (2015) 63 *Clev St L Rev* 495; Ayalew (n 7); W Banks, 'State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0' (2017) 95 *Tex L Rev* 1487.
[12] See M Schmitt, "Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law" (2014) 54 *Va J Intl L* 697; G Bertoli & L Marvel, 'Cyberspace Operations Collateral Damage – Reality or Misconception?' (2017) 2 *The Cyber Def Rev* 53.

Although this literature provides useful insights, it also suffers from considerable limitations. Specifically, in attempting to apply pre cyber era laws to new and rapidly evolving technologies, scholars extrapolate meaning through complicated analyses that reach questionable conclusions. In addition, where scholars are unable to stretch existing law to sufficiently cover a cyber problem, they generally argue that the world must passively await the creation of new norms through state practice.[13] As a result, much of the analyses from this school propagates opaque interpretations and complex interpretive webs that leave significant gaps and raise more questions than they answer.

Among this literature, the *Tallinn Manual 2.0 on International Law in Cyberspace* is arguably the most comprehensive and influential. This tome, which superseded an earlier version focused on jus in bello, is the purposeful product of a conference involving one hundred six scholars, technical experts, and researchers from a wide variety of universities, organizations, and businesses.[14] With its detailed examination of the law pertaining to a range of issues including international human rights, sovereignty, diplomacy, space, and telecommunications, the *Tallinn Manual 2.0* provides an important reference concerning the positions of some leading scholars on international law in cyberspace. At the same time, however, since it does not reflect states' official positions and the conference involved mainly Western scholars, the *Manual* is neither authoritative nor complete.

---

[13] K Mačák, 'From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law, in *Defending the Core: 2017 9th International Conference on Cyber Conflict* 1 (H Rõigas, R Jakschis, L Lindström & T Minárik, eds, 2017); C Lotrionte, "Reconsidering the Consequences for State-sponsored Hostile Cyber Operations Under International Law" (2018) 3 *The Cyber Def Rev* 73.

[14] M N Schmitt & L Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) xii-2.

The other school of thought, which represents a minority view, is that the current international legal regime should not be applied to cyberspace. Rabkin and Yoo, for example, argue that, as with other physical domains, cyberspace should have its own unique framework.[15] From their perspectives, disagreements among legal scholars and their attempts to fit cyber within current international law only create gaps, ambiguity, and confusion.[16]

Unfortunately, while Rabkin and Yoo's argument appears logical on its face, it is based on questionable methods and reaches extreme conclusions. Specifically, the authors posit that, due to lawyers' overreach, international law has become a hinderance to the exercise of U.S. military power. As such, Rabkin and Yoo argue, the international community should adopt a hands-off approach and give the United States carte blanche to operate in cyberspace. This policy, however, would only further encourage malign behaviors, empower a range of actors, and thus likely prove to be counterproductive.

In addition to the above, two other issues plague the literature on cyber operations and international law. First, is definitional inconsistency. Throughout the literature, terms like 'cyberwar' and 'cyberattack' are either defined differently or not at all. As a result, when scholars use the terms in the context of legal interpretations, the conclusions they reach are unclear and often overly complicated.[17]

Second, is the inconsistency between scholars' preferred legal interpretations and actual state practice. Since international law is primarily drawn from conventions and state behaviors,

---

[15] J Rabkin & J Yoo, *Striking Power: How Cyber, Robots, and Space Weapons Change the Rules for War* (Encounter Books 2017) 164-177.
[16] ibid 180-181.
[17] See M Robinson, K Jones & H Janicke, 'Cyber Warfare: Issues and Challenges' (2015) 49 *Computers & Security* 70; Lotrionte (n 14).

these factors are critical elements when discerning applicable legal principles. In the process of attempting to draw the law from pre cyber era conventions and international court decisions, however, scholars often reach conclusions that are contrary to actual state behaviors and preferences.[18] As a result, they obfuscate the path international law in cyberspace should be taking.[19]

Overall, while most scholars argue that current international law applies in cyberspace, fundamental gaps remain over how the provisions should be interpreted. Moreover, rather than mitigating practical problems, much of the literature delves into complex definitional debates or semantic nuances that confound the issues and provide little clarity. In the process, few scholars consider alternative frameworks, arguing that not adopting extant law would leave an unacceptable vacuum.

This approach, however, is shortsighted in that it applies a temporary and insufficient patch that is inconsistent with state practice and fails to address the most prevalent cyber related legal questions. In addition, scholars' passive acceptance that the law will inevitably develop as state practice matures, assumes an outcome that may not occur.[20] Considering that the main state cyber actors have fundamental disagreements over an appropriate regulatory scheme, and the United Nations Group of Experts was unable to reach consensus on a statement for their 2017 findings, the indicators for possible consensus are not favorable. Contrary to most scholars'

[18] Mačák (n 14).
[19] See D P Fidler, 'Just & Unjust War, Uses of Force & Coercion: An Ethical Inquiry with Cyber Illustrations' (2016) 145 *Daedalus, J of the Am Acad Arts & Sci* 37; D Efrony & Y Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *Am J Intl L* 583; Greenberg (n 1).
[20] Tikk (n 11).

claims, therefore, a legal vacuum does exist, and without a change in approach, it is unlikely the void will fill anytime soon.

Legal Frameworks

Over the past twenty-five years, the internet has grown from a relatively small, Western centric platform to a globally integrated web on which most societies rely for their daily functioning. At the same time, cyber technology has infiltrated most aspects of the modern state, as governments, businesses, and individuals have taken advantage of its multiple benefits. These developments have brought dramatic economic, social, political, and physical changes, generated a new valuable commodity in data, and created a vast domain for state competition and conflict.

Despite cyber technology's critical role in modern society, however, international law has failed to keep pace. Instead, the three main cyber actors, Russia, China, and the United States, have been unable or unwilling to agree on an international legal regime.[21] As a result, there are few conventions on the topic and none that directly address key areas of concern such as cyber based attacks and psychological operations.

Unfortunately, this means that, unlike international air travel, finances, communications, and postal deliveries, the internet does not have its own legal code. Instead, as discussed above, most legal scholars argue that cyberspace is regulated by existing international law, which is both amorphous and incomplete. While this has broad sweeping implications for a range of cyber based activities, two issues dominate the literature: the use of force and the principle of nonintervention. To highlight the challenges associated the current legal paradigm in cyberspace, I will look at each of these in turn.

[21] Fidler (n 20); B Mazanec, 'Why International Order in Cyberspace Is Not Inevitable' (2015) *Strategic Stud Q* 78.

Use of Force

Under the United Nations Charter, Article 2(4), states are prohibited from 'the threat or use of force against the territorial integrity or political independence of any state.'[22] Although these words might seem clear on their face, as with any legal treatise they are open to interpretation. Thus, despite extensive analysis by scholars, judges, and officials, the term 'use of force' still lacks a precise definition.[23]

In the cyber domain, this is no less true, as scholars continue to wrestle with the meaning of use of force and the threshold for when a state crosses it.[24] At the same time, however, based on their reading of the United Nations Charter, its travaux préparatoires, and International Court of Justice decisions, most scholars agree on certain criteria.[25] Specifically to qualify as a use of force: 1) a cyberattack must cause physical damage that rises above a de minimis level; 2) the attacker must have an intent to inflict enduring harm; and 3) the attack should be evaluated within the larger context of the states' relationships.[26] Unfortunately, none of these criteria are definitive, which means that deciding whether an attack violates Article 2(4) is situation dependent and subject to interpretation.[27]

---

[22] UN, *Charter of the United Nations* 1 UNTS XVI (1945).
[23] Schmitt, 'The Law of Cyber Targeting' (n 10) 12-18.
[24] A C Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-force' Debate' (2012) 67 *Joint Force Q* 40; I Kilovaty, 'Virtual Violence – Disruptive Cyberspace Operations as 'Attacks' Under International Humanitarian Law' (2016) 23 *Mich Telecomm & Tech L R* 113; Lotrionte (n 14).
[25] R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *J C &* S L 211, 215-217.
[26] Lotrionte (n 14) 75; Schmitt & Vihul (n 15) 333-336.
[27] S Haataja, 'The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach' (2017) 9 *L. Innovation & Tech* 159, 166-168.

Practically speaking, this approach has several critical implications for state behavior in cyberspace. First, it means that disruptive attacks that target critical infrastructure, prevent the functioning of everyday society, put people's health and welfare at risk, and undermine the target state's governance likely do not breach the United Nations Charter if they have no enduring destructive effects.[28] Second, despite data's critical nature and value as a commodity, it is not considered a physical object under the law. Thus, its manipulation or destruction would not qualify as a use of force unless the underlying attack resulted in physical damage to an operating system.[29]

Finally, considering that a target state's response options are largely framed by the nature of the attack, defining use of force narrowly greatly constrains the victim's ability to legally defend itself, particularly if it is unwilling or unable to engage in similar conduct or take action under the restrictive concepts of necessity or countermeasures.[30] As a result, the majority interpretation heavily favors states with more advanced cyber capabilities and encourages aggressive behaviors, which are unlikely to result in negative consequences for the attackers.

Nonintervention

Even if a cyberattack or other event does not cross the threshold for the use of force, it may still violate customary international law if it intervenes in the internal or external affairs of

[28] Buchan (n 26) 217; Intl Comm. of the Red Cross, *International humanitarian law and the challenges of contemporary armed conflicts. Report of the 32nd International Conference of the Red Cross and Red Crescent, Geneva, Switzerland, 08-10 December 2015* (2015). <www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> accessed 21 January 2019, 39-41; Lotrionte (n 14) 78-80.
[29] Schmitt, 'The Law of Cyber Targeting' (n 10); Mačák (n 14).
[30] Schmitt, 'Below the Threshold' (n 13); C Schaller, 'Beyond Self-defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity' (2017) 95 *Tex L Rev* 1619; Lotrionte (n 14) 81-85.

another state.[31] While the criteria for this norm are unclear, scholars agree that to qualify as an unlawful intervention an activity must meet two requirements.[32] First, it must impinge upon the target state's domaine resérvé, or area of authority reserved exclusively for the state by international law.[33] Second, the act must be coercive in that it seeks to compel the target state to adopt certain policies, thereby interfering with its ability to act freely within its due span of authority.[34] Thus, in evaluating whether a state has violated the principle of nonintervention, the focus is not on the target, but rather the sought-after effect. Absent justification, therefore, attacking a commercial entity to compel target state action within its domaine resérvé would violate the principle.[35]

Similar to the use of force discussed above, however, the standards for determining when a nonintervention violation has occurred are limited and nebulous. Specifically, as with most other international legal provisions, the principle applies only to states. Thus, cyber activities conducted by a private organization do not qualify unless they are done at the behest of a government.[36] Although individuals could face domestic legal consequences, absent the host state's cooperation, the realities of jurisdiction, politics, and logistics often mean that perpetrators are beyond the reach of external authorities.[37]

---

[31] Buchan (n 26); UN Grp of Governmental Experts (n 10) 12; W Mattessich, 'Digital Destruction: Applying the Principle of Non-intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage' (2016) 54 *Colum J Transnatl L* 873.
[32] Haataja (n 28) 168-170.
[33] Schmitt & Biller (n 8).
[34] Schmitt & Vihul (n 15) 315.
[35] ibid 315-316.
[36] Lotrionte (n 14) 500.
[37] C Argles, 'A Conceptual Review of Cyber-operations for the Royal Navy' (2018) 3 *Cyber Def Rev* 43, 46-47.

Moreover, even where a state is clearly involved, an attack on commercial organizations or private entities not intended to compel protected state action would arguably be lawful. This requirement not only raises challenges due to the need to demonstrate intent, but it is greatly exacerbated by the entanglement of commercial and governmental cyber infrastructure, which makes it difficult to distinguish between legally protected and unprotected targets.[38] In addition, the limits of a state's domaine resérvé are not clear and they evolve with state practice and opinio juris.[39]

Adding to these challenges, is the question of attribution. Specifically, due to the distributed and complex nature of the internet, cyber actors can readily hide their activities and obfuscate their identities sufficiently to frustrate international accountability mechanisms.[40] While forensic capabilities are improving, malign actors are also becoming more adept at using false flags, off the shelf tools, and other approaches to prevent intelligence organizations from achieving the evidentiary thresholds necessary to support a legally valid and politically supportable response.[41] This combination of challenges not only undermines accountability mechanisms but also encourages cyber actors to be more aggressive.[42]

While it is evident that gaps exist in international law relating to the use of force and the principle of noninterference in cyberspace, it is also important to understand state behaviors,

---

[38] Intl Comm of the Red Cross (n 29) 42.
[39] Schmitt & Vihul (n 15) 314.
[40] G D Solis, 'Cyber Warfare' (2014) 219 *Mil L Rev* 1; Robinson et al (n 18).
[41] T Rid & B Buchanan, 'Attributing Cyber Attacks' (2015) 38 *J. Strategic Stud*. 1; Symantec Corp., *The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks* (3 October 2018) <www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks> accessed 24 February 2019.
[42] A Kozlowski, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (2014) 3 *Eur Sci J* 237.

which are key indicators of how norms are evolving. To provide this information, in the next section I will analyze three cases.

Case Studies

Of the estimated one million cyberattacks that occur each day, most are small scale affairs conducted by state and nonstate actors as protests or probes of security measures.[43] At the same time, however, over the past twenty years there has been a dramatic increase in large, state based operations targeting critical infrastructure, popular sentiments, and political processes.[44] Unfortunately, as reflected above, relevant international law remains nascent, contentious, and deficient in fundamental ways. To evaluate these shortcomings and discern a possible solution, I will examine three cases that are emblematic of how states are acting in cyberspace.

Estonia 2007

In the Spring of 2007, the Government of Estonia decided to move a statue commemorating Soviet losses during World War II from its prominent location to a nearby cemetery. For many Estonians, the statue was a symbol of its fifty year foreign occupation, but for the large Russian population in the country the move was seen as an affront. In response, thousands of Russians rioted in the capital and Estonia suffered unprecedented Distributed Denial of Service (DDoS) attacks on government and private computer infrastructure throughout late April and May.[45]

---

[43] Carbon Black, *Global Threat Report: Year of the Next-Gen Cyberattack*, January 2019 <www.carbonblack.com/resources/threat-research/year-of-the-next-gen-cyberattack> accessed 5 March 2019.
[44] Hathaway (n 9).
[45] E Tikk, K Kaska & L Vihul, *International Cyber Incidents: Legal Considerations* (2010) <ccdcoe.org/library/publications> accessed 18 June 2020, 18-22; Check (n 12) 502-503.

While DDoS attacks use relatively unsophisticated tools to overwhelm web services, they can have dramatic effects when conducted in a coordinated manner against unprotected networks.[46] Since Estonia was one of the most advanced countries in internet connectivity, the DDoS attacks were debilitating, as they interfered with government functions, denied access to banks, blocked emergency services, and cut off communications with the outside world.[47] Further complicating the situation, attribution proved difficult since computers from an estimated 178 countries were involved in the incident.[48] Considering the circumstances and the attacks' technical attributes, however, Estonia argued that they were implicitly if not actively supported by the Russian government.[49]

Although the cyber events did not rise to the level of an armed attack that would implicate NATO's mutual defense provision, questions remain as to whether they violated international law.[50] Assuming the Russian government conducted the attacks, or directed proxies to carry them out, then its behavior would fall under the legal provisions. At the same time, however, since the cyberattacks were not violent or destructive in nature, they did not transgress Article 2(4) of the United Nations Charter.

The other question is whether the attacks violated the principle of nonintervention. Considering that they were part of an effort to compel the government of Estonia to reverse its policy on the statue, an arguable transgression of its domaine resérvé did occur. As such, the

---

[46] J Andress & S Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Elsevier 2011) 176.
[47] North Atlantic Treaty Organization (NATO), Public Diplomacy Division, *Six Colours* (2009) <www.nato.int/ebookshop/video/six_colours/SixColours.html> accessed 22 February 2019; M Shuya, 'Russian Cyber Aggression and the New Cold War' (2018) 11 *J Strategic Security* 1, 4.
[48] Tikk et al (n 46) 24.
[49] Buchan (n 26) 218; Argles (n 38) 46.
[50] NATO (n 48); Tikk et al (n 46) 25.

attacks likely did violate the law if they were conducted at the behest of the Russian government.[51] It is important to note, however, that Estonia did not attempt to hold Russia accountable.[52] Rather, due to attribution challenges, combined with political, strategic, and domestic legal limitations, no punitive action was taken.[53]

Unfortunately, this incident and its outcome set the stage for a growing list of cyber operations by an increasing number of state and nonstate actors. While Russia has been particularly adept at using cyber technology to support invasions and influence operations, others have followed suit.[54] Thus, as will be discussed below, the attacks on Estonia were the first in a long line of operations that have become more aggressive, disruptive, and destructive.

Stuxnet (2009-2010)

In 2010 scientists at the Iranian nuclear enrichment plant in Natanz noticed that the centrifuges used to refine uranium hexafluoride were malfunctioning at an unusually high rate.[55] Over time, multinational computer security forensics analyses determined that the programmable logic controllers regulating the centrifuges' speed were infected with a virus designed to induce destructive vibrations by repeatedly altering their rotation rates.[56]

[51] M Schmitt, 'Classification of Cyber Conflict' 17 (2012) *J Conflict & Sec L* 245, 253; Kozlowski (n 43).
[52] Buchan (n 26).
[53] Tikk et al (n 46) 26-27.
[54] Shuya (n 48).
[55] D Albright, P Brannan & C Walrond, 'Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?' (Institute for Science and International Security December 22, 2010) 1. < https://isis-online.org/isis-reports> accessed 3 August 2020.
[56] K Zetter, 'The NSA Acknowledges What We all Feared: Iran Learns from US Cyberattacks' *Wired* (10 February 2010) <www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/> accessed 21 April 2019.

This virus, known as Stuxnet, was highly complex and uniquely designed to attack Iran's nuclear fuel refinement process by exploiting a Microsoft operating system zero day defect in the centrifuges' programmable logic controllers through a multistep, self monitored, and covert but controlled procedure.[57] Although Iran officially claimed minimal impact, data from the International Atomic Energy Agency and other sources indicate the virus destroyed an estimated one thousand centrifuges, possibly delaying the refinement process two years.[58] Regardless of its impact on the Iranian nuclear program, however, Stuxnet became the first known virus specifically designed and employed to inflict physical damage.[59]

While Stuxnet has not been officially attributed to any state, due to the United States' and Israel's ongoing efforts to undermine Iran's nuclear refinement process through overt and covert efforts, contextual evidence indicates they were involved.[60] In addition, the complexity of the code, precision of its targeting, and clues embedded in the script, such as dates and events important to Jewish history, further implicate the states.[61] At the same time, however, these coding clues could just as well be false flags or contain other meanings that are not immediately evident.[62] Thus, despite years of detective work on Stuxnet, and some well-founded suspicions, attribution remains unresolved.

---

[57] N Falliere, L O Murchu & E Chien, 'W32.Stuxnet Dossier (Version 1.4)' W*ired* (February 2011) <www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf> accessed 27 May 2020.
[58] Albright et al (n 56); Buchan (n 26) 221.
[59] Zetter (n 57).
[60] H Stark, 'Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War' *Spiegel Online* (August 2011) <www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912-2.html> accessed 19 April 2019).
[61] Falliere et al (n 58) 18-24.
[62] Zetter (n 57).

From the legal perspective, there are three important points to consider. First, the lack of attribution raises fundamental questions about whether states were responsible and, thus, if international law even applies. Second, assuming for the purposes of analysis that the US or Israel were involved in the attacks, the next question is whether the Stuxnet incident was an unlawful use of force in violation of Article 2(4). Considering the context and the virus' destructive effects, the attack clearly transgressed the prohibition on the use of force.[63] Finally, if states were culpable, the attack also likely violated the customary law on nonintervention. While this determination is a bit murkier since it is not possible to prove intent, within the context of the attacks it is logical to assume the perpetrators were attempting to undermine Iran's nuclear program, which is within the state's domaine resérvé.[64]

It is unclear, however, if or how Iran responded to the Stuxnet attack.[65] Based on international law, they had at least three options. First, Iran could have responded in kind or through other means as a legal countermeasure to a perceived unlawful act.[66] Based on the criteria for countermeasures, and its complex requirements for prior notice and attribution to a state, however, this route was likely impractical.[67] Similarly, if, as some scholars argue, Stuxnet qualified as an armed attack, Iran could have acted under the doctrine of reprisals.[68] However, it

[63] Buchan (n 26) 220-221; T Payne, 'Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations' (2016) 20 *Lewis & Clark L Rev* 683, 695; Schmitt & Vihul (n 15) 342.
[64] Schmitt & Vihul (n 15) 321.
[65] Zetter (n 57); Buchan (n 26) 226.
[66] Schmitt & Vihul (n 15) 111-134.
[67] G Corn & E Jensen, 'The Use of Force and Cyber Countermeasures' (2018) 32 *Temp Intl & Comp L J* 127.
[68] ibid 342.

would first have had to attribute the Stuxnet attacks to a state and demand that such actions cease.[69] Neither of these approaches was likely feasible under the circumstances.

Finally, Iran could have responded in a punitive or nonpunitive public manner, such as diplomatic protests, an International Court of Justice complaint, or other means designed to gain international approbation against the United States or Israel. Considering the sensitive nature of their nuclear program, and official denial of Stuxnet's impact however, this route would have been impractical as well.

Thus, rather than adopting one of these approaches, Iran appears to have waited two years before taking any significant action against the US. This was likely due to its limited cyber capabilities, which Iran addressed through accelerated efforts to develop a program after Stuxnet.[70] As a result, when Iran possibly did respond by attacking the US banking sector in late 2011-2013, employing waves of DDoS attacks against forty-six businesses, it inflicted millions of dollars in losses.[71] It is important to note, however, that in these and other cyber based operations, Iran has consistently denied any involvement.[72]

US Presidential Election (2016)

In the final months leading to the US presidential election, Wikileaks posted thousands of sensitive documents culled from Democratic National Committee servers through an aggressive,

---

[69] T Anderson, 'Fitting a Virtual Peg Into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals' (2017) 34 *Ariz J Intl & Comp L* 135, 149-152.
[70] C Anderson & K Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Carnegie Endowment for International Peace 4 January 2018) <carnegieendowment.org/> accessed 26 May 2020.
[71] United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, a/k/a 'Nitr0jen26,' Omid Ghaffarinia, a/k/a 'PLuS,' Sina Keissar, and Nder Saedi, a/ka 'Turk Server.' Indictment. 16 Cr 48 (SDNY 21 Jan. 2016).
[72] Efrony & Shany (n 20) 620-623.

yearlong cyber operation.[73] These documents provided damning evidence of party leaders' maneuvers to undermine Bernie Sanders' campaign and raised questions about Hillary Clinton's fitness as a candidate.[74] In the end, the leaks not only created tensions inside the party and damaged Clinton's credibility, but they also exacerbated political divisions within the United States, undermined Americans' faith in the electoral process, and generated a lengthy investigation that continues to rile emotions across the political spectrum.

While the question of who perpetrated the hack and release operation has been a contentious political issue, subsequent forensic analyses by five commercial cyber security firms and the U.S. Intelligence Community concluded that they were conducted by Advanced Persistent Threats (APTs) closely associated with the Russian Government.[75] According to the Director of National Intelligence, the operation had multiple goals, including weakening the integrity of the United States' electoral processes and harming the Clinton campaign.[76] All of these objectives appear to have been met.

Despite the serious effects, however, it is questionable whether the operation violated international law.[77] Specifically, since the attacks resulted in no known physical destruction, they did not contravene Article 2(4). In addition, even though the activities harmed a critical

[73] M Connell & S Vogler, *Russia's Approach to Cyber Warfare* (CNA 2017) 23-24.
[74] Banks (n 12) 1487-1488.
[75] M Buratowski, 'The DNC server breach: who did it and what does it mean?' (2016) 10 *Network Security* 5.
[76] United States Office of the Director of National Intelligence (ODNI), *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections*, 2017.
[77] J D Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 *Tex L Rev* 1579.

component of the US electoral system, an element of the state's domaine resérvé, it was not coercive in nature. Thus, the operation likely did not breach the principle of nonintervention.

Regardless of the legal analysis, six months after the activities were detected the US responded with multiple measures, including targeted economic sanctions, the expulsion of apparent intelligence operatives, and the release of information designed to undercut future Russian cyber operations.[78] For some, however, these actions were deemed insufficient deterrents against such intrusions in the future.[79] Thus, even though it is unclear whether Russia's actions violated international law, the United States' behavior indicates that they were nonetheless unacceptable and mandated substantive, public responses.

Case Analysis

These cases represent only a small sample of the myriad of cyber operations that have been conducted by state and nonstate actors since the internet became publicly available in the early 1990s. At the state level, this includes trillions of dollars in intellectual property theft by the Chinese government, disruptive and potentially destructive cyberattacks against critical infrastructure by North Korea, Iran, and Russia, and extensive psychological operations by Russia against many NATO members and Western aligned countries.[80]

Despite the substantial financial, political, and social costs these activities have inflicted, and the options victims ostensibly have available under international law, however, state

[78] The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (29 December 2016) <www.obamawhitehouse.archives.gov> accessed 17 July 2020.
[79] Banks (n 12) 1491-1492.
[80] P. W. Singer & Emerson T. Booking, *Like War: The Weaponization of Social Media* (Houghton Mifflin Harcourt 2018); Shuya (n 48).

responses have been both constrained and inconsistent with established legal norms. Instead, their behavior reflects a tolerance for low level destruction and costly attacks on banking and other industries. In addition, rather than following the complex legal strictures articulated in the *Tallinn Manual*, states have opted to covertly respond in kind or, in the case of the United States, to apply economic and political pressure where the cyber activities involved electoral manipulation or substantial intellectual property theft.[81]

Collectively, these findings demonstrate that international law is neither constraining nor guiding state behavior in cyberspace, which is rapidly expanding in capability, reach, and complexity. In the face of such a powerful tool, and the apparent unwillingness of the main cyber actors to agree on standards, these developments raise questions about how to create a legal regime that will provide a framework for order in apparent state of chaos.

History of Other Legal Regimes

To discern some principles on how to develop a new legal framework, in this section I will analyze several instructive historical precedents. First, the United Nations Charter on the Law of the Sea (UNCLOS) is arguably one of the most successful and widely followed international legal constructs outside the law of armed conflict. Representing the collective efforts of 150 states engaged in over fourteen years of negotiations, UNCLOS was signed by 119 nations on the day it opened for signature.[82]

[81] Council on Foreign Relations, *A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage* (2018) <www.cfr.org> accessed 2 March 2019.
[82] UN, *The Law of the Sea: United Nations Convention on the Law of the Sea* (1983), xix-xxiv.

At the same time, however, despite this success and the Convention's subsequent ratification by a total of 159 states, it faces some challenges.[83] Specifically, the US has yet to ratify the Convention due to claimed sovereignty concerns, and important bodies of water, such as the South China Sea, remain geopolitical battlegrounds.[84] Still, the US recognizes all but a few provisions as customary international law and most of the maritime territory on the globe is nonetheless successfully demarcated and managed under the UNCLOS regime.

Another successful example is the Convention on International Civil Aviation, also known as the Chicago Convention. Convened in midst of World War Two, the convention initially involved the collective efforts of fifty-five countries united by the recognition that common safety standards were necessary to protect and facilitate flights around the world.[85] These common interests continued to guide the organization after the War, leading to its official entry into force in 1947, and the current involvement of 191 countries.[86] Although periodic accidents do occur, and the law continues to evolve, the Chicago Convention and its associated International Civil Aviation Organization have proven largely successful in setting international standards that ensure billions of commercial passengers travel safely each year.[87]

Finally, a less successful example is terrorism, which has been the subject of decades of failed attempts to develop a holistic framework. While several factors have undermined efforts to

[83] UN Office of Counter-terrorism, *International Legal Instruments* (2019) <www.un.org/en/counterterrorism> accessed 23 April 2019.
[84] M J Kelly, 'Securing Our Navigational Future While Managing China's Blue Water Ambitions' (2012) 45 *Case W Res J Intl L* 461.
[85] International Civil Aviation Organization (ICAO), *Milestones in International Civil Aviation*, (2019) <www.icao.int/> accessed 22 April 2019.
[86] ibid; ICAO, *The History of ICAO and the Chicago Convention* (2011) <https://www.icao.int> accessed 22 April 2019.
[87] ICAO, *Presentation of 2017 Air Transport Statistical Results* (2017) <www.icao.int/annual-report-2017> accessed 23 April 2019.

achieve international consensus on a universal counterterrorism convention, the main point of contention continues to be the criteria for distinguishing among terrorists, members of the armed forces, and insurgents, and how the proposed legal framework should categorize their legal statuses.[88]

In the face of such challenges, states have adopted regional treaties and pursued narrower conventions that address individual elements of the terrorism problem. As a result, there are currently nineteen specialized international conventions and forty-five Security Council resolutions on terrorism, addressing threats to civil aviation, maritime navigation, explosives, hostage taking, financing, and nuclear threats.[89] However, the success of this patchwork approach is questionable considering that terrorism has continued to flourish, with attacks growing from just under 5,000 in 2008 to 10,800 in 2017.[90]

Addressing the Gaps

Based on the above analysis, several findings are evident. First, success in building an international framework has consistently relied upon common interests among the main actors. In the cyber realm, this means that, to develop a universal convention, the United States, Russia, and China would have to reach consensus on a regulatory regime. Considering their political interests in maintaining freedom of maneuver in cyberspace, and differing perspectives on the

[88] UN General Assembly, Sixth Committee: Summary record of the 31st Meeting, UN Doc. A/C.6/71SR.31, 7-8 (02 December 2016) <undocs.org/A/C.6/71/SR.31> accessed 23 April 2019.
[89] UN Office of Counter-terrorism (n 84).
[90] University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism (UMD START), *Global Terrorism Database* (2018) <www.start.umd.edu/gtd/> accessed 3 August 2020.

appropriate model for regulating internet activities, however, this is unlikely to occur. As a result, cyber technology is more closely akin to terrorism than the law of the sea or air travel.

At the same time, however, it is still possible to develop an international legal regime absent a universal convention. Based on the above examples, this would require two supplementary branches. First, although the main cyber actors have significant differences, they also share areas of mutual concern on which to build a consensus. Specifically, as reflected by the Budapest Convention on Cyber Crime and the United States – China agreement on intellectual property protection, common ground might be found in certain segments of cyberspace.[91] While, as with terrorism, this patchwork approach will likely prove insufficient, it will at least start the process of carving out elements of an international regulatory regime.

Second, the United States should engage in a coordinated campaign with likeminded states to purposely develop international legal norms for cyber technology.[92] Although a convention would be the strongest form of international law, where one does not exist, international courts and scholars look to state practice, generally accepted principles, and opinio juris for guidance.[93] Thus, consistent behaviors, and expressed compulsion to follow the attending norms, are the foundations of customary international law.

The United States can use these legal doctrines to its benefit by adopting public policies on cyberspace, acting consistently and publicly along their lines, and expressing the expectation

[91] Tikk (n 11) 8.
[92] B Campbell, 'The Dynamic Evolution of International Law – The Case for the More Purposeful Development of Customary International Law' (2018) 49 *Victoria U of Wellington L Rev* 561.
[93] UN *Charter* (n 23) art 38.

that others act accordingly.[94] By following this approach and working with as many likeminded states as possible to gain consistency in behavior, the U.S. can slowly shape the legal environment. This will not only help fill the current gap in international law but will also set the foundations for a more predictable and stable cyber environment.

Scholars can also play an important role in this process by focusing on the most relevant topics and analyzing state practice to identify patterns of behavior. Thus, rather than debating the threshold for use of force and engaging in tortured efforts to stretch the meaning of pre cyber provisions, scholars should instead focus on identifying and documenting trends in states' strategies, policies, and actions in cyberspace. Among the issues that warrant significant attention are thresholds for attribution, the use of proxies, and how states are responding to cyber based sabotage, espionage, and influence campaigns. By providing relevant analysis on state practice and the norms they are following, scholars can help develop opinio juris, thereby building a crucial body of evidence on evolving norms that courts, international bodies, and policymakers can use to understand how international law is evolving in the cyber realm.

While collectively these efforts will take time to develop a body of law, the approach is consistent with how other international legal regimes have been created. Specifically, UNCLOS rests on maritime customs that evolved over millennia and the Chicago Convention built upon regional frameworks from decades before. Thus, successfully constructing an international legal regime takes time, even when the main actors share mostly common interests.

Rather than following the current paradigm of stretching archaic legal provisions to partially fill a vacuum, therefore, the United States government, likeminded states, and the

[94] M Rinear, 'Armed with a Keyboard: Presidential Directive 20, Cyber-warfare, and the International Laws of War' (2015) 43 *Cap U L Rev* 679, 711.

collective legal community should lead the process of developing a new framework built upon a purposeful effort to form law that accurately reflects state practice and captures the unique nature of cyber technology. Considering what is at stake, and the inadequacy of the current approach, leadership and purposeful action offer the better option.

Conclusion

Over the past twenty-five years, cyber technology has become a central component of modern society. Integrated into a growing array of devices, it has not only greatly increased social connectedness and the utility of products and services but has also increased states' vulnerabilities to external manipulation. As a result, cyberspace has become an increasingly active arena for international conflict, as actors have seized upon the opportunities these developments present. Unfortunately, international law has not kept pace with these changes, as their rapidity and the conflicting interests of key cyber actors have created challenges for the norm and convention development processes.

To address this problem, scholars have attempted to address the resulting gap by arguing that current international law applies to cyberspace. While this makes some intuitive sense, pre cyber era legal provisions often do not translate well to the new technology. As a result, cyber related legal literature contains a complex web of analysis that addresses few of the existing holes and is often inconsistent with state practice. Rather than continuing to follow this paradigm, therefore, in this article I argued for a new approach that accounts for the uniqueness of cyber technology and more aptly reflects state behaviors.

To support this argument, I used a qualitative case study approach that followed four steps. First, I analyzed the literature on cyber technology and the law to identify scholars'

positions and gaps in their analyses. Second, I outlined the extant law relating to two provisions on which most scholars focus: the use of force and the principle of nonintervention. Third, I then applied the current legal interpretations to three cases, Estonia (2007), Stuxnet (2009-2010), and the 2016 United States Presidential Election.

Through this process, I assessed whether these attacks violated international law, how the victim states responded, and whether their reactions were consistent with the *Tallinn Manual*. Collectively, these analyses demonstrated that in the cyber domain the provisions on the use of force and principle of nonintervention are outdated and the remedies for violations largely do not reflect state practice. As such, to guide state decision-making and offer greater predictability in cyberspace, a new legal paradigm is required.

In the fourth step, therefore, I described an alternative approach, founded in part on lessons drawn from the history of how international law developed relating to the sea, air travel, and terrorism. Based on these lessons and my findings, I proposed that, rather than attempting to stretch existing law, the US and likeminded nations should undertake a purposeful effort to develop and enforce appropriate norms, founded on consistent state practice, innovative conventions, and supportive national policies. To support this process, I argue that scholars should conduct relevant research that highlights actual state practice on the most relevant topics and proposes empirically founded legal principles.

As we have seen with other legal regimes, such as those relating to the sea and civilian air transportation, taken together over time these concerted actions can build the appropriate foundational norms and create greater certainty in a highly uncertain domain. Although this process will be challenging and wrought with unpredictability, considering the deleterious

impacts of the existing legal vacuum, the proposal is a much better option than attempting to force archaic legal provisions onto a technology that has far outpaced their utility.