LEGAL CHALLENGES IN THE REALM OF CYBER WARFARE

SHARONA MANN*

Cyberspace is a new dominion that has emerged over the years with the advent of information technology to join the ranks of land, sea, air, and outer space as the fifth domain of warfare. War in this realm poses a threat to all nations of the world, as the remarkable increase in the number of Internet users has opened avenues for malicious entities to launch unprecedented forms of attacks with effects that reverberate around the globe. Cyber warfare has posed many legal challenges that range from the application of the existing international law of armed conflict to regulating the use of advanced cyber weapons in order to prevent incidental loss of life during cyberattacks. This note seeks to analyze five major legal obstacles in the realm of cyber warfare, which highlight the urgency for providing a binding legal framework to cover such attacks and provide mechanisms to counter them. International cooperation also plays a pivotal role in facilitating collective efforts that can prevent the risk of collateral damage during cyber warfare.

I. INTRODUCTION

The world has embraced cyberspace as the new battlefield of war in the twenty-first century, wherein countries use sophisticated software technologies against their foes rather than conventional weapons such as missiles or tanks. The term "cyberspace" was originally coined for a novel written by William Gibson in 1982,[1] but its meaning has since expanded, such that cyberspace is now defined as "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."[2]

In turn, cyber warfare has emerged as a formidable threat to international peace and security because of the increasing dependence of

---

* Sharona Mann is a law student at Amity Law School, Guru Gobind Singh Indraprastha University. Ms. Mann fosters a zeal for the intricacies of international humanitarian law. Her essay entitled *Trafficking of Falsified Medicines* secured second place in the 2018 Surana & Surana International Essay Competition, and her article entitled *Burgeoning Realities of Corporate Social Responsibility in Achieving Global Sustainability* is currently in the process of publication. She would like to extend her gratitude to her parents and Ms. Genivika Mann for their support. She would also like to appreciate Ms. Heather McAdams, Mr. Cole Rabinowitz, Mr. Jackson R. Gandour, and the entire Editorial Board of the *N.Y.U. Journal of International Law & Politics* for their insights and meticulous review of this note.

[1] Thomas Jones, *William Gibson: Beyond Cyberspace*, GUARDIAN (Sept. 22, 2011), https://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace.

[2] U.S. JOINT CHIEFS OF STAFF, JOINT PUBL'N 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 58 (amended ed. 2016).

states on computer networks that support critical infrastructure such as power grids, telecommunication networks, hospital systems, and banking systems. Such dependence increases the likelihood of attacks by "advanced persistent threats" (APTs), i.e., targeted threats undertaken to achieve a specific objective.[3] These APTs can attack the infrastructure of a state, which can cause widespread devastation and give rise to a definite threat to the national security of the targeted state. Moreover, various humanitarian concerns arise when the effects of cyber operations are felt by the public at large. For instance, a cyberattack on the nuclear facility of a country could result in irrevocable damage, ranging from "widespread loss of power" to "uncontrolled release of ionizing radiation."[4]

While cyber warfare has far-reaching ramifications, at the same time, many countries regard it as their preferred mode of warfare. The availability of software to conduct cyber operations and the cost of hiring proxies to carry out attacks against the enemy country demonstrate the cost-effectiveness of employing cyber warfare to accomplish substantial wartime objectives.[5] Countries would certainly prefer this approach due to the involvement of fewer casualties and the reduced financial burden compared to the cost of developing or maintaining conventional weapons for kinetic operations.

Furthermore, cyber warfare provides an advantage to weak and underdeveloped states that lack military primacy or are militarily weak, as they can conduct cyber warfare operations against more technologically advanced states that are increasingly dependent on Internet networks.[6] In the past, small and underdeveloped countries would refrain from launching kinetic operations against their superior adversary due to a lack of sophisticated military equipment. With the advent of cyber warfare, this is no longer the case. An "inverse proportionality" has emerged "between the level of technological advancement of a state and the degree of vulnerability it has."[7]

The critical issue of cyber warfare has also raised a number of legal questions. Chief among these concerns is how law applies to a country's operations in cyberspace. Cyberspace is often considered akin to the American "Wild West," an emanating domain in international relations wherein there are no precise rules to "govern the behavior of states";

---

[3] SYMANTEC, USING SYMANTEC ENDPOINT PROTECTION 12.1 TO PROTECT AGAINST ADVANCED PERSISTENT THREATS (APTS) 4 (2014), https://community.broadcom.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f32e6896-b398-4241-89bc-e6be22d53a6a&forceDialog=0.

[4] CAROLINE BAYLON ET AL., CHATHAM HOUSE, CYBER SECURITY AT CIVIL NUCLEAR FACILITIES 6 (2015), https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.

[5] *Id.* at 5, 9.

[6] KENNETH GEERS, STRATEGIC CYBER SECURITY 10, 98 (2011), https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf.

[7] Afroditi Papanastasiou, Application of International Law in Cyber Warfare Operations 10 (Sept. 8 2010) (unpublished manuscript) https://ssrn.com/abstract=1673785.

further, "[S]uch perceptions of anarchism have bred uncertainty over what is or is not acceptable activity among governments." [8] International humanitarian law (IHL), which consists of rules that seek to limit the effects of armed conflict for humanitarian concerns, has been applied to cyber warfare in an attempt to fill this gap, but legal gray areas have emerged, as cyber operations often do not rise to the level of armed conflict.[9]

The first attempt to crystallize laws concerning cyber warfare was when Professor Michael N. Schmitt, at the invitation of NATO Cooperative Cyber Defense Centre of Excellence, led a group of international law experts in writing the *Tallinn Manual on International Law Applicable to Cyber Warfare* (*Tallinn Manual*); the Tallinn Manual, published in 2013, consisted of black letter laws to be applied to cyber warfare.[10] This was followed by the publication of the second edition of the manual in 2017, the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*), which was greater in scope and application compared to its first edition, expanding the amount of black letter laws to be applied to cyber warfare to 154 rules.[11] Nevertheless, problems still remained.

Unlike the abundant legal literature available on cyber warfare, this note will not attempt to apply existing IHL to cyber warfare, nor question its relevance to cyber warfare. Rather, it will provide a critical analysis of five pertinent legal challenges in the realm of cyber warfare. First, this note will aim to provide a distinction between cyber warfare and cybercrime, as the lack of appropriate usages can impact the legal response of states and their ability to launch countermeasures. This part will also draw a parallel between cyber warfare and information warfare, another frequently used term in cyberspace. Second, this note will focus on the difficulties encountered when applying principles of international law to cyber operations. Third, this note will return focus to the five main pertinent legal issues that have surfaced in the realm of cyber warfare.

II. CYBER WARFARE AND ALLIED CONCEPTS

It is undisputed that technology has become intertwined with everyday life. Almost all individuals regularly engage in a multitude of cyber activities, ranging from online banking to cyber espionage. When studying such activities, the misapplication of related terms can have untoward consequences in the rhetorical debate surrounding cyber operations. For instance, a cyberattack is not the same as cyber warfare, and can only be

---

[8] Levi Maxey, *Tallinn Manual 2.0: Stepping Out of the Fog in Cyberspace*, INDIAN STRATEGIC STUD. (Mar. 9, 2017), http://strategicstudyindia.blogspot.com/2017/03/tallinn-manual-20-stepping-out-of-fog.html.

[9] INT'L COMM. OF THE RED CROSS, CYBERWARFARE AND INTERNATIONAL HUMANITARIAN LAW 1 (2013), https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf

[10] Maxey, *supra* note 8.

[11] *Id.*

called so when it rises to the level of armed attack.[12] Therefore, it is imperative to differentiate analogous terms in cyberspace in order to overcome the challenge of ambiguous terms in cyber warfare, and to ensure an appropriate legal response to them.

The discussion starts with the term "cyber operations," which can be broadly described as "operations against or via a computer or a computer system through a data stream."[13] Such operations can aim to do different things; for instance, they could aim to infiltrate a system and "collect, export, destroy, change, or encrypt data, or to trigger, alter or otherwise manipulate processes controlled by the infiltrated system."[14] Through these means, "a variety of 'targets' in the real world can be destroyed, altered or disrupted, such as industries, infrastructures, telecommunication networks, or financial system."[15] There are multifarious forms of cyber operations, including distributed denial-of-service (DDoS), syntactic, and semantic attacks; however, their examination is beyond the scope of this note. The note will thus proceed by first examining definitions of cyber warfare, then comparing cyber warfare with cybercrime, and finally, drawing a parallel between cyber warfare and information warfare.

A. *Cyber Warfare*

The term *cyber warfare* does not have one universally agreed upon definition, but a number of experts in the diverse academic fields of law, information and communication technology, and military studies have offered definitions. The earliest definition of cyber warfare described those engaging in it as "conducting, and preparing to conduct, military operations according to information-related principles."[16] The term "information-related" refers to a collective hierarchy of data, information, and knowledge.[17] The definition focuses on disrupting, if not destroying, the information and communications systems that the adversary relies upon. This is in line with the main goal of cyber warfare: "turning the 'balance of information and knowledge' in one's favor, especially if the balance of forces was not."[18] However, this definition does not define the full degree of capabilities now possible in cyber warfare: "Limiting the scope of cyber warfare to 'information-related principles' does not

---

[12] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 821 (2012).

[13] Cordula Droege, *No Legal Vacuum in Cyber Space*, INT'L COMMITTEE RED CROSS (Aug. 16, 2011), https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.

[14] *Id.*

[15] Int'l Comm. of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, at 36, 31IC/11/5.1.2 (Oct. 2011).

[16] John Arquilla & David Ronfeldt, *Cyberwar Is Coming!*, 12 COMP. STRATEGY 141, 146 (1993).

[17] *Id.* at 162 n.9.

[18] *Id.* at 146.

describe what happens when an enemy disrupts the electrical power grid of a nation by hacking into the controlling software . . . ."[19]

Another definition that emerged in due course defined cyber warfare as "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state."[20] Such a definition emphasizes an attack on information resident and computer networks, but does not consider the physical destruction that can accompany cyber warfare in the case of attacks targeting critical infrastructure of a state. Yet another alternative provides a state-centric focus on cyber warfare, defining it as the "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[21]

The International Committee of the Red Cross, an international humanitarian institution, states that cyber warfare "refer[s] to means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL."[22] This note follows this definition while further differentiating between related concepts.

The debate around the semantics of cyber warfare has proven never-ending. New connotations are constantly unfolding in order to cover a variety of aspects of the concept, from the authority conducting cyber warfare to the tools employed for advancing it.[23] The obscurity concerning the legal definition of cyber warfare is further evidenced by the *Tallinn Manual*, which does not define cyber warfare, but uses the term "in a purely descriptive, non-normative sense."[24] Hence, it is crucial that the international community develops a legal definition that is acceptable to all states, and that acts as a step towards creation of a binding body of law on cyber warfare.

B. *Cyber Warfare and Cybercrime*

Similar to cyber warfare, *cybercrime* has been defined differently depending on context, due to the absence of a recognized legal definition. In simple terms, cybercrime refers to criminal activity conducted against a computer network, or that which uses the computer as a tool to conduct that activity; it also includes acts against "person, property, government

---

[19] Lionel D. Alford, Jr., *Cyber Warfare: Protecting Military Systems*, 7 ACQUISITION REV. Q. 99, 101 (2000).

[20] Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 AIR FORCE L. REV. 121, 127 (2009).

[21] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 6 (2010).

[22] INT'L COMM. OF THE RED CROSS, *supra* note 9, at 1.

[23] *See supra* notes 20–22 and accompanying text.

[24] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 n.17 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

and society" at large.[25] Some examples include cyberstalking, possession and distribution of pirated software, online fraud, child pornography, and intellectual property crimes.[26] A background paper that was presented at the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders in April 2000 divided cybercrime into two subcategories, providing a sound definition with which the international community may tackle challenges in cyber laws:

> a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
>
> b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network . . . .[27]

After a careful review of both conceptions of the term, the following distinguishing features of cybercrime may be identified:

1. Cybercrimes are mainly profit-oriented, as cybercriminals conduct a variety of malicious activities that can compromise the integrity of computer systems and confidentiality of information. On the other hand, cyber warfare operations are effectuated to achieve a "political or a national security purpose" of a state by undermining the function of a computer network; such operations must also occur within the context of an armed conflict and cross the threshold of an armed attack in order to be called so.[28] However, such qualifying conditions are not relevant with reference to cybercrime.

2. The perpetrators of cybercrime are usually individuals, or companies that hire individuals to conduct nefarious acts; in contrast, cyber warfare is orchestrated by state-sponsored actors or private actors working under the control of the state to fulfill its objectives.[29]

3. Cybercrime involves performing criminal acts that are covered under domestic or international law. For instance, the 2001 Council of Europe Convention, among other international agreements, seeks to regulate and reduce cybercrime.[30] On the other hand, cyber warfare operations are subject to the traditional principles of *jus ad bellum*—the rules governing when a state may resort to war or use armed force—and *jus in bello* or IHL—the rules regulating conduct of parties during armed conflict.[31]

---

[25] Harpreet Singh Dalla & Geeta, Cyber Crime—A Threat to Persons, Property, Government and Societies, 3 INT'L L. ADVANCED RES. COMPUTER SCI. & SOFTWARE ENGINEERING 997, 997 (2013)

[26] *Id.* at 998.

[27] MADHU TYAGI, SECURITY AGAINST CYBER-CRIME 100 (2017).

[28] Hathaway et al., *supra* note 12, at 833 tbl.1.

[29] *Id.*

[30] *Id.* at 862–63

[31] *Id.* at 839, 841.

In many instances, a clear delineation of both cyber warfare and cybercrime is not possible, as they overlap in terms of the means used to fulfill their end goals, even though they may differ in terms of targets and objectives. There are two main instances in which cyber warfare and cybercrime overlap. The first instance is an attack occurring in the context of an existing armed conflict and "undermin[ing] the function of a computer network for a political or national security purpose," but that also violates domestic or international "criminal law (for example, war crimes)" and is "committed by means of a computer system or network."[32] A second overlap involves attacks that "produce effects equivalent to those of a conventional armed attack" and "undermine the function of a computer network for a political or national security purpose", but that are also "violations of the criminal law committed by means of a computer system or network."[33] In any event, a lucid differentiation between both the terms would enable the relevant agencies to deal with both the issues in an appropriate manner.

C. *Information Warfare*

Information warfare in the era of technology utilizes techniques that enable intrusion and disruption of computer systems, along with telecommunications spoofing. "Information warfare" is broadly defined as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[34] The focus of information warfare is achieving information "superiority" in order to support a state's military strategy by protecting its information systems and, at the same time, impacting the information systems of the adversary.[35] This enables the state to develop an accurate picture of the combat situation and place troops respectively. As early as 1995, authors such as Martin C. Libicki had identified seven distinct forms of information warfare: "cyberwarfare," "command-and-control warfare," "intelligence-based warfare," "psychological warfare," "electronic warfare," "'hacker' warfare," and "economic information warfare."[36] Libicki further acknowledged that global information infrastructure had yet to evolve to the point where cyber warfare as a form of combat was possible, and so described it as "a grab bag of futuristic scenarios."[37]

However, at present, cyber warfare has become an intrinsic part of information warfare, as it is used to achieve objectives of a state without using physical force and at a lesser cost. Information is both a tool and a target in cyber warfare, as countries utilize it to spread propaganda and

---

[32] *Id.* at 836.

[33] *Id.*

[34] U.S. DEP'T OF THE AIR FORCE, CORNERSTONES OF INFORMATION WARFARE 3–4 (1995).

[35] *Id.* at 14–15.

[36] MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE?, at x (1995).

[37] *Id.* at x–xi.

conduct false information campaigns. An apt example is Russia, which mounted information operations through media—particularly web-based outlets—against Estonia and Georgia in order to mold the perceptions of the international audience concerning the cyberattacks taking place during the Russian invasion of Georgia in 2008.[38] Moreover, the cyber campaign in Georgia was part of a larger information battle between Russian media and Georgian and Western media for control of the narrative.[39] During this battle, Russian bloggers "flooded" a CNN/Gallup poll with posts stating that "the Russian cause was justified," and also attempted to prevent Georgian media from telling Tbilisi's story.[40] Consequently, such events indicate that information can be manipulated to influence truth, thereby impacting the opinion of the public.

III. THE BEGINNING FOR LAW IN CYBER WARFARE

The first instance in which cyber warfare shook the world was in 2007, when a series of DDoS attacks took place against Estonia, which was implementing the relocation of a controversial Soviet war memorial away from its city center.[41] These attacks crippled the country's government, communication systems, banking systems, and even leading newspaper websites, resulting in the formulation of terms like "Web War I."[42] Likewise, in 2008, Russia launched cyber warfare operations against Georgia that accompanied the ongoing South Ossetia war.[43] These attacks were conducted by botnet, or zombie computers,[44] and brought down official websites of the central government.[45] Yet another major cyber incident took place in 2010, when a form of malware called Stuxnet attacked an Iranian nuclear facility and destroyed its nuclear centrifuges.[46] The events let to publication of several articles applying law of armed conflict (LoAC), or *jus in bello*, to cyber warfare; these scholars primarily focused on the conditions under which cyber warfare could be considered "use of force" or an "armed attack."[47] However, transposition of the preexisting rules resulted in many difficulties, particularly when following the principles of distinction and proportionality.

---

[38] Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, MIL. REV. Nov.–Dec. 2011, at 63, 63–64.

[39] *Id.* at 64.

[40] *Id.* at 65.

[41] Stephen Blank, *Web War I: Is Europe's First Information War a New Kind of War?*, 27 COMP. STRATEGY 227, 227 (2008).

[42] *Id.* at 227,230.

[43] For an explanation of these cyber operations during the Russian invasion of George, see generally Shakarian, *supra* note 38.

[44] *See* Esraa Alomari et al., *Botnet-Based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art*, 49 INT'L J. COMPUTER APPLICATIONS 24, 24 (2012) (explaining that "zombie computers" are "a network of machines with programs . . . and implement[ed] under a command and control (C&C) management infrastructure").

[45] Shakarian, *supra* note 38, at 66–67

[46] Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCE Q. 40, 41, 44 (2012).

[47] *Id.* at 41–42.

The principle of distinction enshrined under Article 48 of the Protocol Additional to the Geneva Conventions (AP I) states that, "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[48] This principle creates two major problems when applied to cyber warfare. First, the interconnection of civilian and military networks makes it hard to differentiate between civilian objects and military objects. Due to the dual nature of cyber infrastructure, civilian networks could also be affected in the event of a cyberattack against military networks.[49] Second, cyber combatants who have technical expertise to launch cyberattacks are starkly different from military combatants who actively participate in an armed conflict. These cyber combatants, when involved in cyber warfare, would be placed outside the protections they enjoy under the LoAC as civilians, which would result in undermining the principle of distinction.[50]

The principle of proportionality implicit in AP I Article 51(5)(b) prohibits "[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[51] However, the weighing of the anticipated military advantage against the incidental loss of life and property is difficult to evaluate because of the nature of cyber warfare. Moreover, it becomes problematic to assess the incidental damage in cyber warfare, as the effects of cyber operations can range from non-lethal to severe. In order to address the diverse challenges posed by IHL, the two editions of the *Tallinn Manual* sought to limit these legal gray areas, but were not completely successful.[52]

IV. THE LEGAL DILEMMAS

The scope and manner of international law's applicability to cyber operations, whether in offense or defense, has remained unsettled since the advent of such operations. After all, when "current international legal norms . . . emerged, cyber technology was not on the horizon."[53] It has therefore become quite important for international law to adapt to the present times in order to deal with the problematic aspects of cyber

---

[48] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[49] *See* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533, 562–66 (2012) (discussing dual-use objects in the context of cyberattacks).

[50] *Id.* at 566.

[51] Additional Protocol I, *supra* note 48, art. 51(5), 1125 U.N.T.S. at 26.

[52] Maxey, *supra* note 8.

[53] TALLINN MANUAL, *supra* note 24, at 3.

warfare, such as by controlling the use of advanced cyber technologies. While judicial interpretation can adapt laws to new situations, this strategy is complicated by the fact that "relevant jurisprudence occurs haphazardly" across diverse jurisdictions, and "it is therefore not always possible to extract a coherent and authoritative interpretation" of the relevant norm.[54] At the same time, newly adapted international norms on cyber warfare require the consent of all the states that choose to be bound by them.[55] However, "such consensus is difficult to achieve," since each state is driven by its own interests and objectives.[56] As cyber warfare seems fraught with problems, this part examines the five most germane issues of cyber warfare.

A. *Equivocal Definitions*

As observed in the first part, the use of interchangeable terms for cyber operations and the absence of a standardized cyberspace lexicon create difficulties in formulating and implementing laws for cyber warfare.[57] In spite of the copious literature on the aforementioned topic, a universal definition has yet to be coined with consensus from the international community. Due to the absence of authoritatively defined terms, different perceptions of the threat hamper concrete cyber security efforts.[58] Therefore, a precise and all-inclusive definition must be devised to bring greater clarity in the international approach towards cyber warfare. This would ultimately enable states to develop a coordinated policy in response to cyber warfare.

B. *A Non-Enforceable Document*

The *Tallinn Manual*, which sought to provide a legal framework for cyber warfare, aimed to produce a nonbinding set of rules that would apply to cyber warfare.[59] The manual expressed the opinion of its drafters, the "International Group of Experts," on various aspects of cyber warfare, but did not have any force of law.[60] A subsequent edition evinced the same intention, stating that the manual was meant to be a reflection of law that existed at the time that it was adopted in June 2016, and was a mere "objective restatement of the *lex lata*."[61] The unenforceability of the comprehensive work creates a hurdle for law in cyber warfare. Moreover,

---

[54] Eitan Diamond, *Applying International Humanitarian Law to Cyber Warfare*, *in* LAW AND NATIONAL SECURITY 67, 69 (Pnina Sharvit Baruch & Anat Kurz eds., 2014).

[55] *Id.*

[56] *Id.*

[57] *See supra* Part II.

[58] NICOLE VAN DER MEULEN ET AL., EUROPEAN PARLIAMENT, CYBERSECURITY IN THE EUROPEAN UNION AND BEYOND 25–26 (2015), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf.

[59] TALLINN MANUAL, *supra* note 24, at 1.

[60] *Id.*

[61] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 2–3 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

countries like China are suspicious of the motives of any effort to build a consensus on the rules of cyber warfare: "As one Chinese media commentary put it," some believe that "the United States is attempting to 'spur the international community into drawing up rules for cyber warfare in order to put a cloak of legality on its "preemptive strike" strategy in cyber warfare.'"[62] In this environment of cynicism, it is important that countries come together to agree on laws regulating cyber warfare on unanimous terms in order to dispel any worries regarding the uniform application of international law.

C. *Problems with General Principles of Law: Sovereignty & Jurisdiction*

Sovereignty in its traditional sense grants a state the ability to exert its authority over its national territory, which encompasses the different domains within that territory.[63] This definition of sovereignty, though, does not provide guidance in cyberspace, as the "[v]iolation of sovereignty is not a useful threshold under current laws and norms for deciding when an event in cyberspace is an act of war or justifies the use of military force."[64] Similarly, the virtual extraterritoriality of cyberspace transcends the boundaries of states. Despite states' apprehensions regarding the independent nature of cyberspace and the difficulty of applying law to such activities, states can and do exert control over the physical infrastructures of cyberspace located within their territory.[65]

The International Group of Experts sought to dispel the apprehensions and provide support to states by noting in both *Tallinn Manuals* that "[t]he principle of State sovereignty applies in cyberspace," with subsequent rules elaborating on this statement further.[66] However, questions are still raised even now regarding the state approach to sovereignty, due to the different stances of states. Observations of state practice show that the principle of sovereignty has been applied differently across the domains of land, air, sea, and space, resulting in disparate legal paradigms.[67] The lack of consistency across these domains makes the formulation of a rule that will apply to cyberspace especially difficult. It appears that states usually apply sovereignty to cyberspace "in a way that does not preclude cyber activities on the infrastructure and territory of another state to include actions . . . that do not impinge on the inherently governmental

---

[62] Julian Ku, *Tentative Observations on China's Views on International Law and Cyber Warfare*, LAWFARE (Aug. 26, 2017), https://www.lawfareblog.com/tentative-observations-chinas-views-international-law-and-cyber-warfare.

[63] TALLINN MANUAL 2.0, *supra* note 61, at 11.

[64] JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, THE "KOREAN" CYBER ATTACKS AND THEIR IMPLICATIONS FOR CYBER CONFLICT 3 (2009).

[65] *Id.* at 3.

[66] TALLINN MANUAL 2.0, *supra* note 61, at 11.

[67] *Id.* at 12 & n.8.

functions of another state."[68] Since states fail to clarify their positions on this issue, the problem remains unsolved.

Another concept connected to the principle of sovereignty is jurisdiction, defined as "the competence of States to regulate persons, objects, and conduct under their national law, within the limits imposed by international law."[69] There are three kinds of jurisdiction under international law: prescriptive jurisdiction, or the ability of a state to prescribe laws; adjudicative jurisdiction, or the ability of a state's courts and tribunals to decide legal cases; and enforcement jurisdiction, or the ability to enforce judgments.[70] "[T]he configuration of cyberspace allows offensive acts to originate, move through cyber space, and affect their targets in ways that are distinctly transnational," creating further problems for determining jurisdiction.[71] There is no doubt that a state can exercise jurisdiction over cyber infrastructure as stated in rule nine of the *Tallinn Manual 2.0*;[72] however, questions arise regarding jurisdiction over cyber activities with only a minimal connection, such as transit of data during cyber operations. As data is transmitted over the fastest routes of the Internet, passing through networks of different countries to finally reach its destination, it becomes difficult to ascertain whether such intermediate countries would be able to exercise jurisdiction.[73] Legal problems also arise while tackling the issue of extraterritorial enforcement jurisdiction, because it is difficult to ascertain the country in which the data relevant to cyber operations resides.[74] States are unbridled when exercising prescriptive jurisdiction over cyber operations within its sovereign territory, but can exercise such jurisdiction extraterritorially only in limited cases, giving due regard to interests of other states.[75] Likewise, both enforcement and adjudicative jurisdiction are limited by consent of the foreign state in whose territory the extraterritorial jurisdiction is sought, keeping in mind the sovereignty of that state.[76] Moreover, there may be overlapping jurisdictions of different states relating to the conduct of cyber activities that could lead to a conflict of laws problem, which can only be solved by a settled international law that clarifies the vexing points of jurisdiction.[77]

D. *International Law of State Responsibility and Attribution*

---

[68] Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 743 (2017).

[69] TALLINN MANUAL 2.0, *supra* note 61, at 51.

[70] *Id.* at 51–52.

[71] Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191, 196–97 (2018).

[72] TALLINN MANUAL 2.0, *supra* note 61, at 55.

[73] *Id.* at 55–56.

[74] *Id.* at 68.

[75] *Id.* at 55–60.

[76] *Id.* at 52–53.

[77] *Id.* at 64.

The *Tallinn Manual 2.0* recognizes another concept key to international law, state responsibility, with respect to cyber activities, especially cyber warfare: As stated in rule fourteen, "[a] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[78] However, this rule is easier stated than applied, as the concept of attribution is not free from problems. The two questions important for attributing cyber operation to a state involve finding the source of the attack and the identity of the perpetrator.[79] Tracing an attack to its source involves many technicalities due to the architecture of the cyberspace, and the "emergence of botnets and malware makes it even more difficult to trace the origin of the attacks/packets."[80] Even when "traced packets are identified, there is no certainty if the right person or location is identified or whether . . . the victim's computer was merely used as botnets."[81] The July 2009 cyberattacks on South Korea and the United States exemplify the difficulty in finding the source of attacks: The initial attack was suspected to originate from North Korea, but subsequent reports revealed that the attacks could be traced to the United Kingdom, Miami (Florida), and South Korea.[82] Furthermore, even if an attack packet can be attributed to the Internet Protocol (IP) address of a host computer, it is difficult to link the IP address to the actual perpetrator. Such "[a] perpetrator can decouple his physical identity from an IP address by using cyber cafes, public Internet facilities (e.g., libraries) and prepaid Internet address cards that can be purchased from service providers without any personal identification."[83] Another important point to note is that the advanced cyber technologies available to belligerents allows them to disguise the location of their attacks, making it seem that the attacks were coming from the cyber infrastructure of another state than the one in which they operate.[84] Therefore, "[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to that State."[85]

Another contentious legal issue is the attribution of the acts of a private actor to a state. States have frequently used proxies to conduct cyber operation against the other states.[86] However, the challenge is how to hold states legally responsible for cyber operations conducted by non-state

---

[78] *Id.* at 84.

[79] *See id.* at 91–92 (discussing the challenges posed by the ability of organizations to disguise their identities or the source of their attacks).

[80] Pauline C. Reich et al., *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents—and the Dilemma of Anonymity*, 1 EUR. J. L. & TECH. 1, 36 (2010).

[81] *Id.*

[82] *Id.* at 14–15.

[83] *Id.* at 37.

[84] TALLINN MANUAL 2.0, *supra* note 61, at 91–92.

[85] *Id.* at 91.

[86] *Id.* at 95.

actors. In accordance with international law, cyber operations conducted by non-state actors, but carried out under the "effective control" of a state, are attributable to the state.[87] The International Court of Justice articulated the effective control test for the first time in the case of *Nicaragua v. United States of America*, in which evidence showed that the United States had financed and organized the Nicaraguan *contras*, and even aided in the selection of targets for *contra* operations.[88] However, the International Court of Justice ruled that the evidence was insufficient to show exercise of effective control by the United States over the *contras*, so the *contra* war crimes that followed could not be attributed to the United States.[89] If such a precedent is extended in the cyber realm, then a state could provide belligerents with cyber tools, identify targets to be attacked, and select the date for the cyber operation to take place, and it would still not implicate state responsibility. This high threshold of attribution impacts the ability of a state to effectively exercise its right of self-defense against the belligerent country, as well as its ability to effectively apply techniques of deterrence, preemption, and proportional response.

E. *Cyber Weapons and Opinio Juris*

Another legal issue of immense importance concerns the state-of-the-art cyber weapons that have become effective tools to advance cyber operations. Traditional international law focused on kinetic weapons, but in the current cyber age,[90] the prevailing international legal frameworks need to evolve in order to regulate the use of sophisticated cyber weapons that pose significant threats to states. Thus, laws need to be kept abreast of developments in cyber technologies. Yet another issue is the secrecy surrounding actions of states in cyberspace. States rarely reveal the development of offensive or defensive capabilities that they undertake for cyber warfare nor do they disclose publicly their legal position or *opinio juris* in relation to cyber warfare.[91] This inhibits any understanding of whether or not states agree with existing efforts to regulate cyber warfare such as the *Tallinn Manual*. Therefore, cyber warfare is surrounded by a "cloud of speculation" about a state's various technological capabilities, offensive or defensive techniques employed in cyber warfare, and views on the legal acceptability of cyber warfare.[92]

V. CONCLUSION

---

[87] *Id.* at 95–96.

[88] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

[89] *Id.* at ¶¶ 115, 276.

[90] Papanastasiou, *supra* note 7, at 13.

[91] Kubo Mačák, *Is the International Law of Cyber Security in Crisis?*, *in* 8TH INTERNATIONAL LAW CONFERENCE ON CYBER CONFLICT 127, 130–31 (Nikolaos Pissanidis et al. eds., 2016).

[92] MYRIAM DUNN CAVELTY, CYBER-SECURITY AND THREAT POLITICS 4 (2008).

The five legal challenges mapped out in this note provide insight into the primary issues that require the attention of the international community when discussing cyber warfare. The first challenge is the absence of a standardized cyberspace lexicon, which creates impediments to formulating and implementing laws dealing with cyber warfare. The second challenge highlighted the unenforceability of the existing framework that applies to cyber warfare. The third challenge involved the complexity in applying the general principles of sovereignty and jurisdiction to cyber warfare. The last two challenges discussed in this note dealt with the broader issues pertaining to international law of state responsibility, attribution, and the secrecy of states with regard to their actions in cyberspace. The world needs to acknowledge the fact that every event occurring in the ubiquitous domain of cyberspace has the ability to affect humanity as a whole. Cyber warfare, like any other type of war, has the capacity to bring humanity to a standstill.

To meet these challenges, a settled legal regime is required that is broad enough to accommodate the developments in cyber operations, but is also precise enough to effectively regulate it. Comprehensive works like the *Tallinn Manual* are a suitable starting point for the creation of an explicit and binding treaty on cyber warfare, the implementation of which would prevent, deter, and mitigate future cyber operations. Therefore, peace in cyberspace is not a distant dream, but one that can be transformed into reality.