FITTING A VIRTUAL PEG INTO A ROUND HOLE: WHY EXISTING INTERNATIONAL LAW FAILS TO GOVERN CYBER REPRISALS

Troy Anderson*

TABLE OF CONTENTS

As nations become ever increasingly more sophisticated, evolving, and adapting along with technology, the rules and international norms that govern interstate interaction must also adapt with the times. Whenever a significant new development in international diplomacy emerges, there is always some residual lag, confusion, and conflict before a new international standard arises to guide that interaction. In recent years, state-on-state cyber-attacks have been one such international development, with government-sponsored malware attacking the interests of other sovereign governments. As with conventional and traditional means of warfare, states have a legitimate interest in deterring other states from engaging in cyber warfare. Because deterrence requires the availability of some form of retaliation or recourse, there is a substantial need for states to know what steps they may take in order to respond to a cyber incursion.

This note will not address the legalities of the initial cyber-attacks; rather, it will focus on the existing body of international law and custom as it relates to retaliation to analyze whether there may be any room in current international law for retaliatory cyber-attacks. This note will conclude that international legal rules are woefully inadequate and incapable of governing cyber retaliation. As a result, a new international convention expressly defining how cyber-attacks fit into existing international law will be necessary.

I. INTRODUCTION

Although state-on-state cyber-attacks have been on the international radar since the late 1990s,[1] their frequency and potency have especially increased in the past several years.[2] Because technology seems to change faster than political systems, the availability and ubiquity of international cyber-attacks has already outpaced the international community's political response.

Put briefly, a cyber-attack is an incursion on electronic or computer systems. Although this Note will not seek to discuss at length the technical intricacies of cyber security, it is useful to have a basic understanding of the types of cyber-attacks employed. Cyber-attacks can be categorized into three broad groups.[3] The first is malware or computer viruses; attacks of this type involve the dissemination of actual software such as Trojan horses and worms.[4] The second category encompasses remote and unauthorized access to computer systems, known colloquially as hacking.[5] The final category, distributed denial of service (DDOS), is perhaps a little bit more complicated and less understood by laypersons.[6] A DDOS attack is essentially an attempt to overwhelm the computing capabilities of a server in which a large number of machines (or potentially limitless number of virtual machines running on a series of powerful computers) simultaneously ping the server, occupying the entire bandwidth.[7] The casual internet user may likely have encountered the results of such an attack in the form of a website being unable to load. While this may seem inconvenient at worst, a well-placed DDOS attack targeting a country or company's infrastructure could cause critical systems to crash and be unavailable in the short term; in cyber warfare, such an attack could be devastating.

---

* J.D. Candidate, 2017, James E. Rogers College of Law, University of Arizona. Special thanks to my wife Elizabeth, herself a brilliant scholar who will soon out-publish me; the board members of the Arizona Journal of International and Comparative Law, with whom it has been a pleasure to work this past year; and to Professor David Gantz, whose insights helped guide the creation of this Note, for their support and assistance throughout the writing process.

1 The first major legal conference on the subject was convened in 1999 by the United States Naval War College. *See* Symposium, *Computer Network Attack and International Law*, 76 NAVAL WAR C. INT'L L. STUD. 1 (2002) (containing the proceedings from the conference).

2 *See generally* Jay P. Kesan & Carol M. Hayes, *Mitigated Counterstrike: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415 (2012).

3 *Id*. at 441 (citing Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyber-attacks: a Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1 (2009)).

4 *Id*. at 441–42.

5 *Id*. at 442.

6 *Id*.

7 Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L. J. 23 (2006).

Unlike nuclear weapons and many other tools of conventional warfare, the programs necessary for cyber-attacks are available to—and used by—many groups besides sovereign states. Some such groups have engaged in cyber-attacks to advance a political agenda,[8] while many others have done so for illicit profit—and yet other groups have committed cyber-attacks merely for sport.[9] There is a large body of academic literature dedicated to such attacks and the associated cyber security measures, including research regarding measures to encourage states to clamp down on cyber terrorists and activists based within their borders; however, such questions are beyond the scope of this note. Instead, this note focuses entirely on state-on-state cyber-attacks, in which the government of the aggressor state creates, funds, or otherwise directs the attack against the assets, interests, or infrastructure of a respondent state.

Although primitive cyber-attacks began to occur in the Cold War (a 1982 CIA operation, for example, led to the explosion of a Soviet pipeline),[10] the advent of the internet and the increased proliferation of computer-based structure has increased the popularity of cyber warfare in recent years. Interstate cyber-attacks began in earnest in 1998, when NATO forces hacked into Serbian air defense programs in order to facilitate bombing raids, and Serbian hackers responded with virus and DDOS attacks of their own.[11] Similarly, Russia employed cyber warfare against Georgian systems during the 2008 Russian intervention in the Georgian provinces of Abkhazia and South Ossetia.[12] Although the specific types of cyber-attacks used are as varied as conventional weapons, it is a safe bet that future wars and conflicts will be accompanied by a cyber element[13] as the United States and other world powers continue to develop and prepare cyber warfare capabilities.[14]

It is worth noting, however, that the Serbia and Georgia examples also involved conventional warfare.[15] In both cases, the digital warfare supported the traditional; even without the cyber-attacks, war still would have ensued. In this way, such cyber-attacks can be viewed as a technological advancement akin to gunpowder, warplanes, or nuclear weapons—merely the next step in the

---

[8] Brian B. Kelly, *Investing in a Centralized Cyber Security Infrastructure: Why "Hacktivism" Can and Should Influence Cyber Security Reform*, 92 B.U. L. REV. 1663, 1667–68 (2012).

[9] *Hackers Knock League of Legends Offline*, BBC (Dec. 31, 2013), http://www.bbc.com/news/technology-25559048.

[10] *War in the Fifth Domain*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792?story_id=16478792&fsrc=rss.

[11] MILAN N. VEGO, JOINT OPERATIONAL WARFARE: THEORY AND PRACTICE 51 (2007).

[12] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[13] *See generally* Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079 (2013).

[14] Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F. L. REV. 121 (2009).

[15] *See* Markoff, *supra* note 12.

development of war technology. Granted, there are new considerations for how the international community will view cyber warfare tactics,[16] but at its core, cyber warfare—as a support tactic employed with conventional warfare—may generally fit into the existing law of war.[17]

Inconveniently for international law, however, cyber warfare has already developed into its own separate entity. States can conduct cyber-attacks against each other's interests without engaging in a conventional war—and indeed, with very few repercussions. Prior to the conflict with Georgia, for example, Russia engaged in a cyber operation against Estonia in conjunction with what was otherwise a simple political conflict regarding the placement of a Soviet-era World War II monument.[18] Estonia was (as are most countries today) highly dependent on its digital infrastructure and was referred to at the time as "the most wired country in Europe."[19] In April of 2007, nearly a month of constant DDOS attacks on various government entities—as well as banks, Internet service providers, and telecommunications companies—severely hampered the Estonian economy and government.[20]

The Estonian incident provided an example of several difficulties in responding to and defending against international cyber-attacks. First, and very importantly, Estonia was not at war at the time, and neither was the attack the opening salvo of a pending conventional campaign or a Pearl Harbor-esque surprise attack.[21] The attacks had very fast results—much faster, for example, than traditional economic sanctions could have had—and all of this was without the commitment or involvement of a full-out assault. Secondly, due to the anonymous nature of the Internet and computer systems generally, it proved extremely difficult for Estonia and its NATO allies to determine definitively the source of the attacks. The Russian government denied any involvement, instead suggesting that the attacks were the work of private, pro-Russian activists.[22] To this day, although it is widely believed that the Russian government was the source (or, at a minimum, acted through proxy organizations), there remains much debate in the international community as to who was at fault.[23] As a result, there

---

[16] Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict* , 32 LOY. L.A. INT'L & COMP. L. REV. 303 (2010).

[17] Nguyen, *supra* note 13.

[18] Ira E. Hoffman, *International Cooperation in Combating Cyber Threats and US Law*, 47 MD. B.J. 36, 38 (2014).

[19] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://archive.wired.com/politics/security/magazine/15-09/ff_estonia.

[20] Hoffman, *supra* note 18, at 38.

[21] Kevin L. Miller, *The Kampala Comrpmise and Cyber-attacks: Can There Be an International Crime of Cyber-Aggression?*, 23 S. CAL. INTERDISC. L. J. 217 (2014).

[22] *Id*. at 223.

[23] Hoffman, *supra* note 18, at 38.

was virtually nothing that Estonia or its allies could do to pursue recompense or retaliate for the attack.[24]

In 2010, another notable cyber-attack occurred when the United States and Israel collaborated on a clandestine digital strike targeted at Iranian nuclear centrifuges.[25] This attack consisted of a malware program infiltration into Iranian systems that caused the slightest changes to the mathematical calculations involved in refining uranium.[26] The program, Stuxnet, was a worm that spread from computer to computer and ultimately affected over 100,000 computer systems.[27] It successfully disabled as many as 1,000 nuclear centrifuges, severely hampering the Iranian nuclear program.[28] Of course, the worm did accompany international economic sanctions as well as a vast body of political rhetoric against the Iranian nuclear program, but it still did not coincide with any sort of conventional warfare. The cyber-attack, by itself, accomplished its goal and demonstrated to the world the possibility of military-grade cyber weaponry.[29]

It is worth noting that despite strong rhetoric and threats of retaliatory cyber-attacks,[30] there was very little actual response from Iran against the United States or Israel. Even though it was widely known that the two states were responsible for the attack, and even though Stuxnet was quite clearly an attack, there proved to be very little that Iran could do to retaliate, at least in the short term.[31]

The problems with cyber security and cyber-attacks generally go beyond the mere technological capabilities of governments to attack each other or to defend against such attacks. It is possible that Iran, Estonia, and Georgia were simply unprepared technologically to retaliate, but it is just as likely that they were rather unable to retaliate, given the general confusion regarding what options are available for a retaliating state.[32]

---

[24] *See id*.

[25] Jordan Peagler, Note, *The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law*, 31 ARIZ. J. INT'L & COMP. L. 399 (2014); *A New Kind of Warfare*, N.Y. TIMES (Sept. 9, 2012), http://www.nytimes.com/2012/09/10/opinion/a-new-kind-of-warfare.html.

[26] John Markoff, *Malware Aimed at Iran Hit Five Sites, Report Says*, N.Y. TIMES (Feb. 11, 2011), http://www.nytimes.com/2011/02/13/science/13stuxnet.html [hereinafter Markoff, *Malware*].

[27] David Z. Bodenheimer, *Cyber Warfare in the Stuxnet Age: 10 Cannonball Law Keep Pace with the Digital Battlefield?*, A.B.A. SCITECH LAW, vol. 8 no. 3, 2012, at 4.

[28] Manny Halberstam, Note, *Hacking Back: Reevaluating the Legality of Retaliatory Cyber-attacks*, 46 GEO. WASH. INT'L L. REV. 199 (2013).

[29] Bodenheimer, *supra* note 27, at 5–6.

[30] *Id*. at 5.

[31] *Id.*

[32] *See* Sklerov, *supra* note 3, at 2 ("As warfare changes, so must the law, and warfare is changing fast.").

II. THE INADEQUACY OF CONVENTIONAL DETERRANCE

States cannot employ deterrence to protect themselves against cyber-attacks from other governments. Effective deterrence requires the legitimate threat of adequate reprisal against a rational actor;[33] if states are not able to threaten retaliation, deterrence is simply not possible.[34] Critically, the unavailability of deterrence as a strategy substantially destabilizes the international political community. This is one of many reasons why international law regarding cyber retaliation must be improved.

When the invention of nuclear bombs led to the massive arms race of the Cold War, the retaliatory capabilities of nuclear states kept the peace by way of the looming threat of annihilation if a state were ever to go on the offensive.[35] The infamous concept of mutually assured destruction represents, perhaps, the most obvious and effective example of deterrence in international politics: if the state were to launch an attack on another state, either the attacked state or its allies would be able to respond in kind with overwhelming nuclear force.[36] The efficacy of the initial attack would be small consolation for the aggressor state after it was itself destroyed in the retaliatory attack. Despite the availability of thousands of nuclear warheads (and an abundance of mutual hatred, including a number of proxy wars), the Cold War never erupted into a nuclear holocaust, due, in large part, to the effectiveness of nuclear deterrence and mutually assured destruction.

Deterrence also works in conventional warfare; one state may be unwilling to attack another because of the possibility of reprisal. Deterrence works in economics, where the threat of international sanctions can provide incentive for states to play fair. In fact, deterrence works in any field where a party's actions could lead to negative consequences. Cyber warfare represents a unique situation in deterrence where widespread uncertainty leaves rational actors guessing as to what a response will be to aggression. In part, this is intentional; after all, the very nature of cyber-attacks is clandestine so that if a state knows that a cyber-attack is coming, the attack will be much less effective; a nuclear bomb, on the other hand, is no less explosive when its existence is known.[37] However, because even countries themselves remain uncertain as to how they would

---

[33] Austin Long, *Deterrence: The State of the Field*, 47 N.Y.U. J. INT'L L. & POL. 357 (2015).

[34] Frank C. Zagare, *Reconciling Rationality with Deterrence: A Re-examination of the Logical Foundations of Deterrence Theory*, 16 J. THEORETICAL POL. 107 (2004).

[35] Gary Schaub, *When Is Deterrence Necessary? Gauging Adversary Intent*, STRATEGIC STUD. Q., vol. 3 no. 4, 2009, at 4.

[36] Long, *supra* note 33.

[37] *Id*. at 375.

respond to a cyber-attack,[38] deterrence would have a difficult time working in cyber warfare.[39]

It should be noted that deterrence does not necessarily require a cyber-attack reprisal. On the contrary, ideally, the strongest deterrence would be legal recourse in the International Court of Justice or perhaps by way of strong international sanctions. However, as demonstrated by the Estonia, Georgia, and Iran incidents, there are several reasons why this is especially difficult. In the first place, it is often difficult to ascertain definitively who was responsible for a cyber-attack.[40] If a respondent state cannot identify a cyber-attack's aggressor, it would be especially difficult for that state to overcome the burden of proof in an international court. This is not a problem for most conventional warfare:

> In a kinetic war, the foe is usually obvious, as satellites and electronic signatures unmask the country that launched the missile or fired the shot. With cyber war, the opposite is true. Cyber weapons may bounce from botnet to botnet across multiple international borders, leaving questions about whether terrorists, organized crime, or unfriendly countries launched the assault.[41]

In addition to the difficulties in pegging the culprit, there is actually no specific international convention designed to deal with cyber-attack claims—and cyber warfare is far too new for any customary law to have been established. Neither has any cyber case been previously decided in the International Court of Justice (ICJ) or other significant international tribunal. Under the current system, states would be left to attempt to fit a cyber claim into laws that were designed for physical incursions; that law is simply not prepared to deal with cyber warfare. Therefore, the best solution for cyber deterrence—which will help to stabilize the turbulent world of rapidly promulgating cyber technologies—is for the United Nations to establish clear guidelines for how states may respond, including how states may pursue justice in international courts or from the international community.

---

[38] Ryan Lucas, *Government Mulls How to Deter Cyberattacks*, CQ ROLL CALL, 2015 WL 4258495 (last visited Oct. 21, 2016).

[39] *See* Kesan & Hayes, *supra* note 2.

[40] *But see* Yoram Dinstein, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Conference*, 89 INT'L L. STUD. 276, 279 (2012).

[41] Bodenheimer, *supra* note 27.

III. EXISTING OPTIONS FOR RESPONSE

Traditional deterrence of conventional attacks or unfriendly acts can be divided[42] into four basic doctrines of international law and custom: retorsion,[43] countermeasures,[44] reprisal,[45] and *jus ad bellum*.[46] Each of these doctrines originated in a world without cyber-attacks and reflects an international system quite different from the modern day.[47] Accordingly, either a UN resolution, or new international convention must present new definitions and guidelines governing definitively how retaliatory cyber-attacks would fit into these categories. This note will therefore analyze the efficacy and legality of retaliatory cyber-attacks that fit into each of the systems.

A. Retorsion

Retorsion is "an act of lawful retaliation in kind for another country's unfriendly or unfair act."[48] It is the most innocent, innocuous, and ineffective type of retaliation that a state can take. It is unique among retaliatory actions in that it is always lawful. Unlike the other categories of deterrence, retorsion is not an exception to international law that allows states to commit illegal actions; rather, retorsion is an unfriendly but otherwise legal action.

Retorsion usually is diplomatic or economic in nature, rather than militaristic. Examples of retorsion include: cessation of trade (that has not been contracted in an international agreement), suspension of diplomatic relations, and expulsion of diplomats, travelers, and other nationals of the country retaliated against; [49] a quintessential example is found in the Obama administration's expulsion of Russian diplomats in response to the Russian cyber-attack of

---

[42] It is important to note that the lines between these different doctrines are often quite blurred; there was no founding document that created these doctrines or carefully delineated and categorized them into distinct concepts. Accordingly, different sources sometimes use the terms interchangeably or with different meanings than are used in this note.

[43] Sklerov, *supra* note 3, at *36.

[44] G.A. Res. 56/83, U.N. Doc.. A/RES/56/83, Articles on Responsibility of States for Internationally Wrongful Acts (Dec. 12, 2001) .

[45] GARY D. SOLIS, THE LAW OF ARMED Conflict 318 (2010).`

[46] Steven R. Ratner, Jus Ad Bellum *and* Jus In Bello *After September 11*, 96 AM. J. INT'L L. 905 (2002); Frederic Megret, *The Relationship Between* Jus Ad Bellum *and* Jus in Bello*: Past, Present, Future*, 100 AM. SOC'Y INT'L L. PROC. 121 (2006).

[47] Bodenheimer, *supra* note 27.

[48] *Retorsion*, BLACK'S LAW DICTIONARY 1342 (10 ed. 2014).

[49] *Id.*

hacking.[50] Any of these actions would generally be legal, though unfriendly, without specific justification under any circumstances. The defining characteristic of retorsion is that it is an act that breaches no duty and breaks no laws. A state can never be sued in an international court or tribunal for committing retorsion, as there is nothing illegal about such a course of action.

As a retaliatory action, retorsion can never apply the "use of force,"[51] as prohibited by the UN Charter.[52] The precise meaning of this phrase has been debated throughout the lifespan of the United Nations, particularly in recent years as it relates to cyber warfare.[53] Although some argue that the phrase refers exclusively to the use of *armed* force,[54] there has nevertheless been continuing debate on the point.[55] The classical debate on this issue is exacerbated by the onset of cyber warfare, which is an entirely new element to consider. After all, the entire difficulty with defining the legality of retaliatory cyber-attacks comes from the fact that cyber-attacks do not function as a conventional use of force, but

---

[50] David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), http://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

[51] U.N. Charter art. 2, ¶ 4. In its entirety, the provision reads: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

[52] This section of the Charter also is a violation of the purposes of the United Nations, which are defined as follows in Article 1: "1. To *maintain international peace and security*, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace; 2. To *develop friendly relations among nations* based on respect for the principle of equal rights and *self-determination of peoples*, and to take other appropriate measures to strengthen universal peace; 3. To achieve *international co-operation* in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and 4. To be a center for *harmonizing the actions of nations* in the attainment of these common ends." U.N. Charter art. 1 (emphasis added). Although an extremely strict reading of Article 2(4) could suggest that the action not in harmony with the Purposes would be an unlawful act and that, therefore, any action that does not strive to maintain the peace, develop friendly relations, and achieve international cooperation would be unlawful. However, this would mean that virtually all acts of retorsion, unfriendly by nature, would be illegal under the Charter, and it has not been interpreted as such. Although it is possible for cyber-attacks to be considered illegal because their purpose is not consistent with Article 1, this interpretation is unlikely to take effect.

[53] *See, e.g.,* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 656–74 (2012).

[54] *Id*.

[55] GEORG KERSCHISCHNIG, CYBERTHREATS AND INTERNATIONAL LAW 62–63 (2012).

nevertheless achieve a similar result.[56] Additionally, that the language of the UN Charter did not specify *military* force implies that it recognizes the possibility of nonmilitary actions rising to the level of the use of force.[57] Such actions would be illegal by the same rule.[58]

Of course, the provision concerning the use of force is not the only international law that could be broken in a retaliatory measure; in order to be legal (and qualify as retorsion), an action must also comply with the prohibition against intervention in a state's sovereign affairs.[59] Article 2(1) of the UN Charter states that the entire United Nations is based upon the "sovereign equality" of member states.[60] The International Court of Justice (ICJ) has interpreted this to mean that states are prohibited from acts that interfere with each other's internal or external affairs, including, for instance, a nation's political process.[61] This principle against intervention in sovereign affairs is, according to the ICJ, "part and parcel of customary international law."[62] As such, violation of this principle is necessarily illegal, and therefore, retorsion must not rise to the level of intervention, even indirectly.[63]

Because retorsion exclusively involves actions that are not illegal, the decision of when retorsion is justifiable is not a matter of law.[64] Generally, however, proportionality comes into play.[65] Although the actions taken are legal regardless of the circumstances, they are defined as retorsion when they are taken in response to an act by another state.[66] In practice, retorsion is usually undertaken in response to actions that are, themselves, unfriendly but otherwise legal;[67] however, this does not have to be the case.[68] Retorsion need not be

---

[56] INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 32 (Michael N. Schmitt ed., 2013). [hereinafter TALLINN MANUAL].

[57] Halberstam, *supra* note 28.

[58] *Id.*

[59] TALLINN MANUAL, *supra* note 56, at 44.

[60] U.N. Charter art. 2, ¶ 1. *See also* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

[61] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. Rep. 14, ¶ 205 (June 27) [hereinafter Nicar. v. U.S.]. This principle also draws upon the concepts in Article 1(2), which refers to a respect for the "self-determination of peoples." U.N. Charter art. 1, ¶ 2.

[62] Nicar. v. U.S., 1986 I.C.J. at ¶ 202.

[63] TALLINN MANUAL, *supra* note 56, at 44.

[64] 2 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 37 (1921).

[65] *Id*. at 44.

[66] MALCOLM N. SHAW, INTERNATIONAL LAW 1022 (5th ed. 2002).

[67] *Id*. This reflects the concept of proportionality. States that are greatly wronged by an illegal act are more likely to retaliate using one of the more severe methods, such as countermeasures or reprisals, because those actions may be legally justified at that point. Still, it is within the purview of the state to stick with retorsion even when reprisal may be an option.

justified by "circumstances precluding wrongfulness" because retorsion does not involve wrongful acts, and this is its defining characteristic.[69]

The tradeoff, of course, is that retorsion is generally considered to be a very weak form of retaliation, as evidenced by its description as a "method of showing displeasure."[70] Retorsion is merely "discourteous or unkind,"[71] akin to a "fail[ure] in comity or politeness."[72] It involves what the International Law Commission calls "simple measures."[73] Although retorsion can sometimes include economic sanctions and secession of trade, the parties involved are members of the World Trade Organization, they remain subject to its regulations, and as a result economic retorsion is generally limited.[74]

The efficacy of retorsion also highly depends upon the relative power of the states. For example, when Ceylon (present-day Sri Lanka) nationalized American oil assets, the United States responded by suspending all foreign aid to that country.[75] Because the United States is not legally required to provide such aid, this act was one of retorsion. Consider, however, if the roles were reversed: Ceylon could not have suspended foreign aid to the United States because Ceylon was the recipient, not the benefactor—and even if Ceylon were providing aid to the United States, the disparate economic power of the two states would surely make Ceylon's hypothetical suspension of aid less impactful. Because of the comparative power of the United States in this situation, it was able to perform an unfriendly but legal act that was actually detrimental to the interests of Sri Lanka. In this way, only states in a position of relative strength are generally able to come up with effective methods of retorsion. This is one of the biggest weaknesses of the strategy in general: legal methods of retaliation are generally only available to relatively powerful states.[76]

---

[68] JAN KLABBERS, INTERNATIONAL LAW 168 (2013). There is some debate in academia on this point. Some scholars believe that retorsion may only be in response to an illegal action. Other scholars believe this distinction is unnecessary. For our purposes, the retorsion is in response to a hypothetical cyber-attack that is presumed to be illegal; it is therefore senseless to further divide retorsion into additional categories.

[69] *Id*.

[70] SHAW, *supra* note 66, at 1022.

[71] OPPENHEIM, *supra* note 64, at 36.

[72] *Retorsion*, *supra* note 48, at 1342 (quoting THEODORE D. WOOLSEY, INTRODUCTION TO THE STUDY OF INTERNATIONAL LAW 188 (5th ed. 1878)).

[73] MATH NOORTMANN, ENFORCING INTERNATIONAL LAW: FROM SELF-HELP TO SELF-CONTAINED REGIMES (2005).

[74] Roberto Echandi, *Non-Compliance with the Words: the Remedies of Customary International Law*, 106 AM. SOC'Y INT'L L. PROC. 118, 120 (2012).

[75] C.F. Amerasinghe, *The Ceylon Oil Expropriations*, 58 AM. J. INT'L L. 445–46 (1964).

[76] Of course, this problem is not unique to retorsion—any method of retaliation is more effective coming from a position of strength. Still, this demonstrates one of the reasons that retorsion is an unsatisfactory general solution as a deterrent for cyber incursions.

Justifying retaliatory cyber-attacks under the doctrine of reprisals is difficult. Because retorsion cannot be an otherwise illegal act, the retaliatory attack must not violate international law. Employing retorsion as a retaliatory measure need not be in response to an illegal act, so a state may argue that cyber-attacks are not a violation of international law in order to justify its actions under the doctrine of retorsion. However, this would necessarily preclude the state from arguing countermeasures, reprisal, or *jus ad bellum* as a justification for the response, since each of these types of retaliatory deterrence requires first the commission of an unlawful act.

In analyzing whether a cyber-attack falls in line with international law, the first step is to determine whether the attack constitutes the use of force.[77] This would of course depend on the nature of the attack. Any use of malware, for example, would more likely be viewed as a use of force, especially if the intent of the malware is to disrupt or destroy critical systems or assets. A DDOS attack would be somewhat easier to justify because the damage caused is ultimately reversible. Even so, it would nonetheless require an attack on the other state's systems, which would lend credence to the argument that such an attack would rise to the level of a use of force. However, hacking may not amount to the use of force,[78] even if it involves bypassing firewalls and other security protocol, because cyberspace—unlike land, sea, or airspace—is not considered sovereign territory under current international law.[79] As such, hacking would not be necessarily illegal and would not represent the use of force.

The Tallinn Manual[80] states that a retaliatory cyber-attack violates the prohibition against the use of force "when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[81] This line of thinking essentially reimagines the cyber-attack as a conventional action and asks whether the attack would be a forceful intrusion. Stuxnet, for example, destroyed centrifuges and other scientific equipment.[82] It is therefore more similar to a targeted airstrike than to espionage operations, and it would likely qualify as a use of force.[83] Stuxnet and similar cyber-attacks cannot therefore be classified as retorsion because they violate the prohibition against the use of force.

---

77 Halberstam, *supra* note 28, at 213.

78 TALLINN MANUAL, *supra* note 56, at 45.

79 An analysis of the costs and benefits of creation and implementation of new international law regarding sovereignty of cyberspace is, unfortunately, beyond the scope of this note.

80 The Tallinn Manual is a publication by a group of experts making policy guidelines for NATO regarding the use of cyberwarfare. TALLINN MANUAL, *supra* note 56, at 1.

81 *Id.* at 45.

82 Markoff, *Malware*, *supra* note 26.

83 TALLINN MANUAL, *supra* note 56, at 45.

Many cyber operations that would not involve the use of force, however, would violate the second step in the analysis: the prohibition against interference.[84] An operation, for instance, that does not destroy any property or systems, but seeks instead to disseminate information or undermine public confidence in a regime would likely constitute a breach of sovereignty. Although the "mere intrusion into another State's systems does not violate the non-intervention principle,"[85] if the effect of the cyber operation is coercive, the act is illegal. In other words, the cyber element of the action does not immunize the response from being illegal or allow it to qualify as retorsion if the operation has the same ultimate fact as actions that have, in the conventional sense, been traditionally considered to be interference, such as those intended to bring about regime change.[86]

If cyber operations are off the table for retorsion, traditional acts of retorsion would be much less effective. Responding to a cyber-attack by expelling diplomats would be dissatisfying, to say the least, for many states. The traditional inefficacy of retorsion coupled with the difficulties in even tracing cyber-attacks to a specific government entity means that, if a retaliatory cyber-attack cannot fit within the definition of retorsion, that retorsion itself is an unsatisfactory legal framework for cyber deterrence.

Limiting a cyber operation to the confines of legality in order to allow it to qualify as a legal retorsion severely limits the power of the cyber operation. This, in turn, drastically lowers the viability of cyber retorsion as a method of deterrence. Furthermore, whether a retaliatory cyber-attack is benign enough to be legal—and therefore to qualify as retorsion—remains undecided in the international community. The doctrine of retorsion is, therefore, unable to provide sufficient guidance or deterring power for states considering retaliatory cyber operations.

B. Countermeasures

Countermeasures[87] represent a different type of unilateral action taken in response to an incursion or unfriendly act.[88] Whereas retorsion involves unfriendly but otherwise legal acts, a countermeasure, as defined in international

---

84 *See generally* Nicar. v. U.S., 1986 I.C.J. Rep. 14 (June 27).

85 TALLINN MANUAL, *supra* note 56, at 44.

86 *Id*.

87 Some authors do not draw a distinction between countermeasures and reprisals. *See, e.g.*, Halberstam, *supra* note 28, at 208, n.61. Similarly, "countermeasure" is a term used frequently in a political, economic, or military context to refer generically to a retaliation. However, this note will use the term to refer specifically to countermeasures as defined by the UN International Law Commission.

88 Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 14 (2011).

law, amounts to the failure to fulfill an international obligation.[89] Whereas retorsion must involve actions that would never be illegal, countermeasures may include certain specific illegal actions.[90] Although the doctrine of countermeasures can be difficult to apply to retaliatory cyber-attacks, international law spells out the doctrine more thoroughly than the concept of retorsion, and it is therefore important to explore in order to understand the legality of retaliation under international law.

The UN International Law Commission published a document on the responsibility of states that defines countermeasures and sets forth guidelines for identifying legal and illegal countermeasures.[91] This document provides a specific body of law to which states may look in analyzing whether a retaliatory measure is legal. However, while the document legalizes and gives credence to a variety of retaliatory measures, ultimately, it also provides a number of restrictions.

The first of these restrictions is that a state may only employ countermeasures in response to "an internationally wrongful act."[92] To some extent, this is self-explanatory: by definition, an action can only be a countermeasure where it is taken in response to another action. However, this definition is crucial not as a limitation on the action itself, but rather as a prerequisite for conducting a countermeasure. Whereas retorsion is necessarily legal, a countermeasure is only permissible when it complies with these restrictions. As such, a state performing a countermeasure must first be able to show that the aggressor state has committed a "wrongful act."[93]

Furthermore, the scope of a countermeasure is limited to actions intended to compel the aggressor state to resume lawful actions and make amends for its wrongful act.[94] The actions must similarly allow the other state to return to legal activity. Therefore, a countermeasure does not serve as an opportunity to get back at an aggressor state, but is rather specifically limited to actions that will compel that state to resume lawful activity. In this way, countermeasures are a prime example of deterrence. However, countermeasures are limited in that if the aggressor state ceases its attack, the responding state must, by law, also cease its countermeasures.[95]

---

89 U.N. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter Draft Articles].

90 *Id*.

91 *Id.*

92 *Id*.

93 *Id*.

94 Draft Articles, *supra* note 89.

95 TALLINN MANUAL, *supra* note 56, at 37.

The third restriction—and most difficult to reconcile with a retaliatory cyber-attack—is that actions are "limited to the non-performance for the time being of international obligations."[96] In general, this restriction means simply that a state may, as a countermeasure, temporarily withdraw from treaties or renege on its promises. However, nothing in the ILC's document suggests or allows that states may employ the use of force or breach the sovereignty of another state as a justifiable countermeasure.

As a result, in terms of cyber retaliation, countermeasure options are quite limited. Although some scholars interpret countermeasures as justifying retaliatory cyber-attacks,[97] it is difficult, if not impossible, to define a DDOS attack or bit of malware as the mere temporary non-performance of an obligation. Although there has not yet been an example of an international dispute regarding this issue, it is unlikely the state would be able to use the document countermeasures as defined by the ILC as a legitimate justification for the commission of a retaliatory cyber-attack.

C. Reprisals

The next two existing legal frameworks (reprisals and *jus ad bellum*, or justification in war) walk a fine line in international law—the line between a "use of force" and an "armed attack." Critically, there yet remains substantial debate in the international community as to where those lines are drawn, and the question of what sort of actions fall into which category is, as yet, unresolved. The recent introduction of the additionally obfuscating question of cyber operations further confuses a delicate area of international law already rife with blurred lines.

Unlike a countermeasure or retorsion, a reprisal involves the use of force. Whereas a countermeasure, as defined in international law, is an otherwise-illegal action that nonetheless may not involve arbitrary interference or any force by the responding country, reprisals may be quite extensive in their aggression and even violence. However, reprisals necessarily fall short of all-out war.

The law of reprisals, in addition to stemming from a long-standing international custom, finds its legal home in a disputed gap between two terms in the UN Charter. Article 2(4) prohibits the "use of force" by states.[98] The Charter does not define the term. As discussed above, cyber-attacks do not necessarily fit clearly into this definition, either. Certainly, most cyber incursions do not involve the physical trespass and destruction envisaged in the era of kinetic warfare in which the Charter came to be. However, it is without doubt that some cyber operations are capable of undertaking a level of destruction consistent with the phrasing as a use of force.

---

96 Draft Articles, *supra* note 89.

97 *See, e.g.*, TALLINN MANUAL, *supra* note 56, at 45; Hinkle, *supra* note 88, at 14.

98 U.N. Charter art. 2(4).

This prohibition against using force ceases to take effect, however, in instances of self-defense. Article 51 of the Charter guarantees that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[99] Armed attacks, then, absolve a state of its Article 2(4) obligation not to engage in the use of force against another state. However, critically, the Charter does not employ the same language in both sections—the "use of force" in one and "armed attack" in the other.

Impliedly, then, the Charter leaves a gap where states could be victims of the use of force not rising to the level of an armed attack. In such a situation, the victim state would remain unable to respond with force because Article 51 would not yet exempt them from Article 2(4). The doctrine of reprisals fills this gap, allowing states to use force in kind as a response to the use of force, so long as neither the initial action nor the response rise to the level of an armed attack.

There exists substantial debate and discrepancy between states regarding the existence of this gap or even the legal justifiability of the doctrine of reprisals. The United States, for instance, does not agree that the different language in Articles 2(4) and 51 describe different types of actions.[100] However, as pointed out by one distinguished professor of international law, the Charter was "one of the most carefully crafted instruments in the history of international law," and the difference in the wording could not therefore have been an accident.[101] Different scholars and different organizations often differ as to whether and how the Charter limits proportional responses.[102]

The difference between the use of force and an armed attack has not always been intuitive. This was an issue, for example, in the International Court of Justice decision in *Nicaragua v. U.S.*, in which the ICJ decided that the United States' actions could not be justified because a "mere frontier incident" did not qualify as an armed attack to justify setting aside Article 2(4).[103] Furthermore, the Eritrea-Ethiopia Claims Commission held that violent border clashes and cross-border incursions did not qualify as armed attacks, limiting severely the legality of responses.[104]

Furthermore, there exists a discrepancy between stated international law and actual practice of members of the United Nations Security Council and other member states.[105] Notwithstanding the apparent legal conundrum caused by the

---

[99] U.N. Charter art. 51.

[100] Dinstein, *supra* note 40, at 279.

[101] *Id*.

[102] *See* Sklerov, *supra* note 3.

[103] Nicar. v. U.S., 1986 I.C.J. Rep. 14, ¶ 103 (June 27); *see also* Dinstein, *supra* note 40, at 279.

[104] Eritrea-Ethiopia Claims Commission, Partial Award, Jus ad Bellum, 45 I.L.M. 430, 433 (Hague 2006).

[105] William V. O'Brien, *Reprisals, Deterrence, and Self-Defense in Counterterror Operations*, 30 A. J. INT'L L. 421, 421 (1990).

gap between Articles 2(4) and 51, states tend to respond to force with force.[106] As a result, the foundation for the legality of forceful reprisals stems not from the language of the United Nations charter, but rather, from the custom of states—making forceful reprisals especially difficult to justify as a legal recourse in international law.

In any event, reprisals need not necessarily amount to the use of force as prohibited by the Charter.[107] Instead, "economic and political coercion"—and, potentially, limited cyber-attacks—could be the kind of per se illegal response justified as a reprisal.[108] Such non-forceful reprisals enjoy a more grounded legal framework, but accordingly must comply with existing precedent.[109] Specifically, the ICJ laid out the three-part test for reprisals in *Gabcikovo-Nagymaros Project:*[110]

> In the first place it must be taken in response to a previous international wrongful act of another State and must be directed against that State . . . . Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it . . . . [Third,] the effects of a [reprisal] must be commensurate with the injury suffered, taking account of the rights in question.[111]

In these restrictions, reprisals are similar to countermeasures, as discussed above, with the notable exception that they are not limited to the nonperformance of existing obligations. The question of legality surrounding the use of force notwithstanding, reprisals must nevertheless be limited to the scope of responding to a wrongful act by another state, must have followed diplomatic communication, and must be proportional to the initial wrong.[112] Some scholars interpret these limitations further, noting that if an offending state were to

---

[106] Derek Bowett, *Reprisals Involving Recourse To Armed Force*, 66 AM. J. INT'L L. 1, 1 (1972).

[107] Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: The Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 220 n.89 (2002).

[108] Sklerov, *supra* note 3, at 37.

[109] *Id*. at 36–37.

[110] Note that the ICJ, in this decision, uses the term "countermeasure" to refer to what this Note calls non-forceful reprisals, distinguishing from countermeasures as described by the Draft Articles. *See* Draft Articles, *supra* note 89. *Gabcikovo-Nagymaros Project* predates the draft articles, which is why it does not use the same terminology. Still, this discrepancy is an example of why express new agreements are necessary instead of piecemeal assembly of the law from disparate sources.

[111] Gabcikovo-Nagymaros Project (Hung., v. Slovk.), Judgement, 1997 I.C.J. Rep. 7, ¶ 83–85 (Sept. 25).

[112] *Id*.

discontinue its violation of international law, the responding state would not then be justified in enacting its reprisal.[113]

This framework is somewhat nonsensical in the cyber context. The idea of discontinuing cyber-attack, for example, would almost never be practical for most malware or DDOS attacks; most of the damage would have been done in the opening salvo. By the time a responding state can take the slow, deliberate measures required by the ICJ's three-part process, the damage to infrastructure and systems would have significantly worsened. Furthermore, attribution issues would make it difficult for states to prove in a court context that the aggressor state had committed an internationally wrongful act, as states must do if they wish to rely on legal reprisals that they would defend in court.

All of this is further complicated by the debate surrounding the definitions of the use of force and armed attacks in the UN Charter. If the Eritrea-Ethiopia Claims Commission found that bloody firefights did not amount to armed attacks, then some states may assume that they have substantial latitude in defining their own cyber-attacks as forceful responses not rising to the level of an armed attack. Similarly, however, states may view cyber-attacks as non-forceful in general.

Additionally, because the idea of reprisals is not rooted in the express terminology of international law but instead in international custom, individual states may take widely disparate views of when and how they may employ reprisals as a justification for cyber-attacks. The lack of any definitions to clarify the application of reprisals in a cyber context dramatically complicates application of reprisals in governing retaliatory cyber-attacks.

D. Jus ad bellum

The broadest options for retaliatory cyber-attacks are available under the law of war—and accordingly, retaliatory cyber-attacks grounded in the law of war have a proportionally stringent threshold for justification. Scholarship and real-world examples of lawfulness in warfare are plentiful;[114] as they relate to cyber-attacks, the same rules that govern conventional warfare apply. *Jus ad bellum* and its counterpart *jus in bello* are the international doctrines governing lawfulness entering war and lawfulness in warfare, respectively.[115] Both are complex, and both apply to cyber as well as kinetic warfare.

Although warfare long predated the establishment of the United Nations, the modern legal framework for the law of war stems from the Article 51 preservation of states' rights to employ the use of force in order to act in self-

---

[113] Halberstam, *supra* note 28, at 218 (citing YORAM DINSTEIN, WAR AND SELF-DEFENSE 249 (5th ed. 2012)).

[114] *See, e.g.,* Frederic Megret, *Jus in Bello and Jus ad Bellum*, 100 AM. SOC'Y INT'L L. PROC. 121 (2006).

[115] *See id.*

defense.[116] Once a state is the victim of an armed attack, it may reply in kind. Alternatively, a state may employ force when authorized by the UN Security Council.[117]

Some states and scholars argue that the right to self-defense includes the right to preemptive strikes[118]—or "anticipatory self-defense,"[119] as they are more innocuously designated.[120] Anticipatory cyber-attacks in retaliation for a cyber-attack that has not yet occurred could be justified under the same logic.[121] However, other scholars point to the express language of the UN Charter in contending that anticipatory attacks are incompatible with *jus ad bellum*.[122] The ICJ has demonstrated a reluctance to decide one way or another whether anticipatory self-defense is generally justifiable.[123]

Either way, there must have been either an actual armed attack or an imminent armed attack in order to justify forceful reprisals under the law of war. In the cyber context, it is not clear when a cyber-attack rises to the level of an "armed attack"[124]—indeed, even in kinetic warfare, this definition is elusive.[125] Definitional issues aside, there would yet remain endless options for aggressor states to pursue cyber operations that do not rise to the level of an armed attack, effectively tying the hands of would-be respondent states.[126]

Because there is no separate body of law or agreed-upon definition regarding cyber-attacks, a retaliatory cyber-attack is only justifiable under *jus ad bellum* if a conventional attack would also be justified in that situation. After all, with *jus ad bellum*, states cross the threshold into all-out war. In international relations, cyber warfare is not a separate entity—"it is just ordinary warfare with a little bit of extra."[127] It is not necessarily a separate type of warfare, but rather, a separate type of weapon.[128]

As such, if a responding state invokes *jus ad bellum* appropriately, it is not limited merely to a retaliatory cyber-attack, but may additionally employ any conventional weaponry that is permissible under *jus in bello*.[129] There have not yet been any wars fought exclusively in cyberspace, though cyber warfare suites

---

[116] U.N. Charter art. 51.

[117] U.N. Charter arts. 39–42.

[118] *See* Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699 (2005).

[119] *See* Jensen, *supra* note 107, at 217.

[120] Sklerov, *supra* note 3, at 33–36.

[121] *Id*.

[122] Dinstein, *supra* note 40, at 278.

[123] Halberstam, *supra* note 28, at 212; Nicar. v. U.S., 1986 I.C.J. Rep. 14, ¶ 176 (June 27).

[124] Hinkle, *supra* note 88, at 11–12.

[125] *See* Eritrea-Ethiopia Claims Commission, *supra* note 104.

[126] Hinkle, *supra* note 88, at 12.

[127] Dinstein, *supra* note 40, at 283.

[128] *Id*. at 281.

[129] *Id*. at 280.

have been involved in conventional wars. The conflicts in Serbia and Georgia have shown that, in practice, once states are at war, cyber-attacks are also on the table.[130]

Because retaliatory cyber warfare is governed by the same law of conflict as conventional warfare, it still must conform to a number of conditions. For example, cyber warfare may not specially target civilians.[131] Indeed, multiple early treaties and conventions banned the targeting of civilians in warfare.[132] Although many types of malware and hacking operations would be able to specifically affect only military targets, other cyber-attacks, including DDOS or attacks on infrastructure, could have severe enough effects on civilian populations to violate *jus in bello*. Thus, though retaliatory cyber-attacks justified under *jus ad bellum* have more freedom than retorsion, countermeasures, or reprisals, they are still somewhat restricted.

Modern-day states and international tribunals have demonstrated a reluctance to apply the laws of war. All-out warfare is—and should be—a last-ditch defense for states. It is difficult to justify, requiring not merely a use of force, but an armed attack (or its cyber equivalent). Indeed, it is not clear that there has ever been a cyber-attack that would, on its own, constitute an armed attack that would invoke *jus ad bellum*. Accordingly, *jus ad bellum* is severely lacking as a primary framework governing states' legal options in responding to aggressive cyber intrusions or attacks.

IV. IMPLICATIONS

A. The Need for New Law

There has never yet been a case before the ICJ or any similar international court deciding how retaliatory cyber-attacks fit into existing international law. Neither has there been any international convention, UN resolution, or wide-reaching treaty to clarify how retaliatory cyber-attacks implicate existing legal frameworks. Instead, the entire body of scholarship on the issue is speculative, simply proposing potential arguments that states could make in the case of a cyber-attack. And if scholarship is purely speculative and deeply divided, so, too, are the current doctrines of states. As noted, the United States, for instance, does not recognize the distinction between the use of force and an armed attack.[133] Accordingly, there is no international agreement as to the threshold that would justify the different levels of retaliatory cyber-attacks discussed in this Note.

---

[130] *See infra* section I.

[131] Some scholars disagree. *See* Kesan & Hayes, *supra* note 2, at 500.

[132] Michael A. Newton, *Reconsidering Reprisals*, 20 DUKE J. COMP. & INT'L L. 361, 373 (2010).

[133] Dinstein, *supra* note 40, at 279.

Perhaps most illustrative of this problem is the disparity between the Tallinn Manual[134] and the UN's Draft Articles[135] on State Responsibility regarding countermeasures. The Tallinn Manual is a NATO policy guide advising states on legal frameworks for retaliatory cyber-attacks, and it contains a valuable set of rules by which to assess cyber operations. However, in its analysis of what the UN General Assembly has permitted for countermeasures, the Tallinn Manual ignores a critical limitation.[136] Its proposed Rule 9 on Countermeasures cites to and incorporates many of the Draft Articles' limitations on permissible countermeasures, including that the countermeasure must be designed to compel the offending state to resume compliance with its obligations.[137] It does not, however, discuss the implications of Article 49(2) of the Draft Articles, which state that "countermeasures are limited to the non-performance for the time being of international obligations."[138] Because a cyber-attack is usually not a mere non-performance of an international obligation, the retaliatory countermeasures described by the Tallinn Manual may not actually be legal.

It is possible that, in a future case, a responding state following the Tallinn Manual's Rule 9 may convince the ICJ or other tribunal that a retaliatory cyber-attack is justified as a countermeasure under the draft articles. The reality is, however, that at present, even the most comprehensive state guide on the legality of retaliatory cyber operations may not be describing operations that would actually be legal.

As a result, international law governing cyber-attacks is dangerously unclear. As cyber warfare capabilities become ever more advanced, the risk of highly damaging cyber-attacks increases. Because states and scholars do not agree as to how existing law governs such cyber-attacks, states have very limited options for deterrence, retaliation, or defense. The result is widespread insecurity and instability.

B. A Simple New Framework

The solution is not complicated, though it would be difficult to implement. The primary difficulty surrounding the application of existing law to retaliatory cyber-attacks resides in the difficulty of predicting how the international community will view the various definitions involved with retaliatory measures. At a basic level, however, the foundation does already exist for comprehensive and binding guidelines for state responses to cyber-attacks by another state.

---

134 TALLINN MANUAL, *supra* note 56.
135 Draft Articles, *supra* note 89.
136 TALLINN MANUAL, *supra* note 56, Rule 9.
137 *Id*. Rule 9(3).
138 Draft Articles, *supra* note 89, at 49(2).

Some scholars have dismissed the necessity or efficacy of a new treaty regarding cyber warfare as a mere repetition of the existing law of armed conflict.[139] This, however, is precisely the greatest strength of a new treaty as a solution to the legal quagmire that is the law of retaliatory cyber-attacks. States are likely to be reluctant to agree to sweeping new restrictions on the use of cyber-attacks; indeed, three of the states that have been the most important actors in international cyber-attacks—the United States, Russia, and China—are also three of the permanent members of the UN Security Council. However, new guidelines would not necessarily limit the options for states in responding to cyber incursions. Instead, adopting a clear legal framework would protect both powerful and weak states.

Such new definitions could be implemented in any of four ways with approximately equal effect. Firstly, states could convene an international convention, as has been done many other times in response to many other threats.[140] Secondly, a resolution from the United Nations General Assembly, similar to the Draft Articles on State Responsibility, would provide a sufficient basis for the application of definitions to retaliatory cyber-attacks. Such a resolution could then evolve into a formal international convention. Similarly, a resolution from the UN Security Council could provide guidance, especially given the Security Council's responsibilities in overseeing the use of force internationally.[141]

However the new legal framework is implemented, it should focus on two new guidelines. First, it should establish when the initial attack rises to the level of a use of force—or even an armed attack. Such guidelines would signal to states whether they are limited to retorsion and countermeasures or may advance to the more extensive reprisals and cyber warfare. In this, the Tallinn Manual's analysis of the use of force in cyber-attacks will prove useful.[142] It uses an effects-based analysis: a cyber-attack amounts to the use of force "when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[143] Such an approach is not overly complicated, but it is nonetheless not currently accepted as international law; adopting this rule would drastically simplify the analysis for responding states to determine their course of action.

The second area of focus should be on the acceptable responses available to attacked states. This section should reiterate the UN Charter's right to self-defense while also clearly establishing the very high threshold required to invoke that right. It should also apply the standards of the *Gabcikovo-Nagymaros Project* decision and the Draft Articles on State Responsibility in limiting the scale and

---

139 Dinstein, *supra* note 40, at 286.

140 Consider, for example, the 1999 International Convention for the Suppression of the Financing of Terrorism as an example of states coming together to establish basic guidelines to combat a modern threat.

141 *See* U.N. Charter arts. 39–42.

142 TALLINN MANUAL, *supra* note 56, Rules 10–17.

143 *Id*. Rule 11.

aims of appropriate retaliatory cyber-attacks. Finally, it should emphasize the general principles of attribution, necessity, and proportionality as binding on any retaliatory measures.

With these guidelines, the international community could very easily modify existing law to fit the changing realities of modern warfare. These proposed guidelines are not a radical new system—radical changes would be as difficult to implement as they are unnecessary. However, without such changes, states are still left without clear legal guidelines governing the new reality of state on state cyber-attacks.

IV. CONCLUSION

The existing laws that govern legal retaliations and deterrence come from an era of entirely different warfare. A century ago, state borders were physical, state interests were tangible, and state-on-state attacks involved formal militaries—or, at a minimum, physical weapons. Today, states exist with one foot in the physical world and one in the virtual. This is a trend that is likely to continue. Because of the volatile nature of cyber warfare, and because the existing body of law is woefully inadequate in governing these issues, it will be necessary for these nations to take steps to modernize the doctrine of reprisals in order to reflect the new technological challenges facing the world today. Individual states may have substantial reservations about limiting their options by agreeing to the creation of a new international cyber warfare regime. The clarity that would come with a new, binding, international convention, however, would bolster states' cyber defenses by enabling the deterrence of cyber-attacks. As such, updating international law is critical to maintaining stability in the virtual world—and peace in the real world.