

Cyber Attacks and the Beginnings of an International Cyber Treaty

STEPHEN MOORE†

I.	Introduction	224
II.	Framing Questions for an International Cyber Treaty.....	228
	A. A Growing International Industry.....	228
	B. Is Customary International Law Sufficient?.....	230
	C. What are the Benefits of an International Cyber Treaty?	231
III.	Customary International Law and Cyber Warfare	232
	A. The Need to Define.....	232
	B. Customary International Law	234
	1. Jus Ad Bellum	235
	i. The Use or Threat of Force.....	236
	ii. Exceptions to the Use or Threat of Force	237
	2. Jus in Bello	239
	i. Distinction	239
	ii. Proportionality	240
	iii. Neutrality	241
IV.	Cyber Treaty Bare Bones	241
	A. Initial Concerns for a Definition.....	241
	B. Attribution: State and Non-State Actors	242
	1. State Actors.....	243
	2. Non-state Actors	243
	C. Responding to Cyber Attacks: U.N. Security Council, Self Defense, and Countermeasures.....	246
	D. Enforcement: Reparations and Compliance.....	249
V.	Is an International Cyber Treaty Feasible?.....	250
	A. Conflicting International Interests and Technology Dependence.....	251
	1. Identifying Interests of the Key Players	251
	2. Technological Dependence.....	253
	B. Agreement to Move Forward.....	254

†J.D. Candidate 2014, University of North Carolina School of Law. I am grateful for the expertise of Professor Scott Silliman in both framing and reviewing this note. Thank you too to my wife, Heather, for your unwavering love, support, and copy editing skills.

VI. Conclusion256

“Because of the interlocking nature of major global financial institutions, including individual banks, even a cyber attack on one nation’s financial infrastructure could have a fast-moving ripple effect, undermining confidence globally.”

Richard A. Clarke¹

“When the centrifuges first began crashing in 2008 at the Natanz enrichment center, the crown jewel of the Iranian nuclear program, the engineers inside the plant had no clue they were under attack. That was exactly what the designers of the world’s most sophisticated cyberweapons had planned.”

David E. Sanger²

“Today, as nations and peoples harness the networks that are all around us, we have a choice. We can either work together to realize their potential for greater prosperity and security, or we can succumb to narrow interests and undue fears that limit progress.”

President Barack Obama³

I. Introduction

The helicopters hummed along the broken Pakistani terrain, their mission accomplished.⁴ Osama Bin Laden was dead and the entire SEAL Team Six crew was safe.⁵ In three and a half hours the team had entered Pakistani airspace, assaulted the compound in Abbottabad, and returned to Afghanistan, all before the

¹ RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 246 (2010).

² DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA’S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 188 (2012).

³ PRESIDENT OF THE UNITED STATES OF AMERICA, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 3 (2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter WHITE HOUSE STRATEGY].

⁴ See SANGER, *supra* note 2, at 97.

⁵ *Id.* at 103.

Pakistani government was ever aware of the incursion.⁶ The Pakistani air defense never detected the helicopters in its airspace.⁷ Some speculated it was this inability to detect U.S. forces that most damaged U.S.-Pakistani relations, more than the actual invasion of Pakistani territory.⁸ “Never had the [Pakistani] military, the strongest institution in the country, been so humiliated since it lost three wars to India.”⁹ Programmers and hackers stationed at U.S. Cyber Command in Ft. Meade, Maryland, could have contributed to the undetected incursion, using cyber technologies to infiltrate and turn off Pakistan’s air defense system simultaneous to the U.S.’s physical assault.¹⁰

It would not be the first such cyber attack. In 2007, Israeli bombers flew undetected into Syria, blowing up what was later determined to be a partially completed, North Korean-built nuclear enrichment facility.¹¹ The bombers flew undetected not due to some new radar-absorbing technology,¹² but because Israel used a

⁶ *Id.* at 103. (“‘We [do not] think the Paks saw us until we were over the border again,’ one American official told [Sanger]. The whole process—in and out of country—had lasted about three and a half hours, and the Pakistanis had still not scrambled any forces.”). Ultimately, two MH-60 Black Hawk helicopters and two MH-47 Chinooks entered Pakistan air, all undetected by Pakistani air defense. *Id.* at 97-103.

⁷ *Id.* at 97. It is reported that Pakistan merely had its radar turned off. *Id.* at 97 (“‘It was a little like us on Pearl Harbor Day – they had their radar off,’ one of Obama’s aides told me later. ‘It was the first of several examples of incompetence that broke our way.’”).

⁸ *Id.* at 105 (“‘With every new detail [of the raid]—how long the SEALs were inside Pakistan, how they refueled on Pakistani territory without being detected—the television commentators in Islamabad stoked the public anger.”). Ultimately, the leaders of the Pakistani military and intelligence service were subjected to eleven hours of hearings before the Pakistani parliament, resulting in “a resolution condemning the Abbottabad raid as a violation of sovereignty and a demand for a review of the partnership with the United States ‘with a view to ensuring Pakistan’s national interests were fully respected.’” *Id.* at 107-08.

⁹ *See id.* at 105-06.

¹⁰ *See generally* SANGER, *supra* note 2, at 263-64 (explaining U.S. Cyber Command).

¹¹ *See* CLARKE & KNAKE, *supra* note 1, at 2-4.

¹² *See id.* at 5 (“‘Those aircraft, designed and first built in the 1970s, were far from stealthy. Their steel and titanium airframes, their sharp edges and corners, the bombs and missiles hanging on their wings, should have lit up the Syrian radars like the Christmas tree illuminating New York’s Rockefeller Plaza in December. But they didn’t.’”).

complex cyber attack to mask its entry.¹³ Israeli programmers manipulated Syria's air defense¹⁴ so that it would fail to report anything on the radar.¹⁵

Israel and the U.S. often share new technologies as part of their strong relationship in developing cyber weapons.¹⁶ In 2007, both nations joined together to initiate "Olympic Games"—in part an effort to "cripple, at least for a while, Iran's nuclear progress" through the use of their combined cyber capabilities.¹⁷ Olympic Games used a series of computer worms to progressively infiltrate and seize control of computers in the highly secretive Natanz nuclear enrichment facility in Iran.¹⁸ Eventually, the worm was used to physically alter critical components within the nuclear facility.¹⁹ To purify uranium into a usable energy source for nuclear power, and potentially nuclear weapons, rotors within centrifuges must spin the uranium at the speed of sound.²⁰ The surreptitious worm was engineered to spin the delicate centrifuges too fast or too slow, ultimately causing them to break apart.²¹ The worm reportedly caused nearly a thousand centrifuges to fail,²² greatly delaying Iranian efforts to enrich uranium.²³

If the U.S. used such cyber attacks against Pakistan during the

¹³ *Id.* at 5-8.

¹⁴ Syria's air defense, notably, was Russian-built. *Id.* at 5.

¹⁵ *Id.* at 5-8.

¹⁶ *See id.* at 8 ("Whatever method the Israelis used to trick the Syrian air defense network, it was probably taken from a playbook they borrowed from the U.S."); *see also* SANGER, *supra* note 2, at 195 ("Soon the American and Israeli intelligence partnership kicked into high gear. Olympic Games became part of the weekly conversation between security officials from the two countries, conducted over secure video lines and with visits to Washington and Jerusalem.").

¹⁷ *See* SANGER, *supra* note 2, at 190.

¹⁸ *See id.* at 188-89.

¹⁹ *See id.*

²⁰ *See id.* ("It was particularly difficult to manufacture the delicate rotors at the center of the machines. The rotors are the most vital single part: they spin at terrifying speeds, and each rotation of each centrifuge creates a slightly more purified version of Uranium-235.").

²¹ *See id.* at 189 ("[Rotors] are very temperamental. Spin them up too quickly and they can blow apart. Put on the brakes too fast and they get unbalanced. When that happens, the rotors act like a metallic tornado, ripping apart anything in its way.").

²² *See id.* at 206 ("In Natanz, 984 centrifuges came to a screeching halt.").

²³ *See* SANGER, *supra* note 2, at 189.

Bin Laden raid, as developed in conjunction with Israel, what are the international implications? What would limit the U.S. or any other country from using these technologies solely for such a unique scenario? What would keep them from using it to mask planes flying over Iran? What if another country, perhaps China, developed such a capability and used it to hide a Pearl-Harbor level initial strike against a smaller national entity, like Taiwan?

Similar attacks have already occurred. In 2008, a seven-day conflict between Russia and Georgia witnessed the widespread use of cyber attacks by “hacktivists” in Russia, which brought Georgian governmental websites offline.²⁴ What limits cyber attacks to military targets? Estonia, a highly technological country, was brought to its knees by a series of attacks in 2007 that initiated in Russia and greatly disrupted Estonia’s banking systems.²⁵ Similarly, during the 2008 Georgia-Russian conflict, cyber attacks were used to shut down Georgia’s banking and mobile phone systems.²⁶ What limits cyber attacks to state actors? What is the appropriate response if groups such as Al Qaeda or Anonymous²⁷ initiate cyber attacks against a state or international

²⁴ See CLARKE & KNAKE, *supra* note 1, at 20; see, e.g., Mark Clancy, *Arm Yourself for Cyber War—Are You Next?*, 2012 SIBOS CONFERENCE PANEL (DTCC, New York, N.Y.), http://www.dtcc.com/news/sibos/Clancy_SIBOS.pdf (addressing the term “hacktivists” and their role in cyber warfare) (last visited Sept. 30, 2013).

²⁵ CLARKE & KNAKE, *supra* note 1, at 12-16 (“Estonians could not use their online banking, their newspapers’ websites, or their government’s electronic services.”). See also Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151, (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy et al. eds., 2010) (“The impact of the cyber assault proved dramatic; government activities such as the provision of State benefits and the collection of taxes ground to a halt, private and public communications were disrupted and confidence in the economy plummeted.”).

²⁶ See CLARKE & KNAKE, *supra* note 1, at 20 (“The attacks triggered an automated response at most of the foreign banks, which shut down connections to the Georgian banking sector. Without access to European settlement systems, Georgia’s banking operations were paralyzed. Credit card systems went down as well, followed soon after by the mobile phone system.”).

²⁷ “Anonymous is not a group, but rather an Internet gathering.” *ANON OPS: A Press Release Dec. 10, 2010*, ANONNEWS (Dec. 10, 2010), <http://anonnews.org/?p=press&a=item&i=31>. “Anonymous is not a group of hackers. We are average Internet Citizens ourselves and our motivation is a collective sense of being fed up with all the minor and major injustices we witness every day.” *Id.*

organization?

These are only a few of the issues impacting the international community as it comes to terms with the growing technological dependency of states and the resulting dramatic impact of cyber attacks. This note is organized into four parts, resulting in the suggestion of an initial framework for an international treaty governing cyber attacks. Part I develops the basic questions surrounding an international cyber treaty, demonstrating several potential benefits of an international accord. Part II discusses customary international law that implicates cyber attacks. It focuses on both *jus ad bellum*, the international legal framework that governs the escalation to and initiation of war, and *jus in bello*, the international legal framework that governs once war has begun. Part III addresses the major concerns of an international treaty. It discusses in turn definitional issues, attribution, self-defense, and enforcement. Part IV highlights the feasibility of an international treaty, focusing on varying national perspectives, interests, and potential complications.

II. Framing Questions for an International Cyber Treaty

The growing international interest in the creation and use of cyber weapons increases the likelihood that states and non-state actors will provoke the ire of one another.²⁸ Such provocation could easily spark conflict unless tamped down by some overarching set of rules or understanding as to what cyber tools or actions are admissible, as well as to some real method of enforcement.²⁹ A cyber treaty may be a useful tool to step into the current void in customary international law, bridging the gap between state interests.

A. A Growing International Industry

The scale and scope of the growing field of cyber security

²⁸ See, e.g., David M. Herszenhorn et al., *With Snowden in Middle, U.S. and Russia Joust, and Cool Off*, N.Y. TIMES, June 25, 2013, http://www.nytimes.com/2013/06/26/world/snowden.html?pagewanted=all&_r=0 (noting the increased hostility between the U.S., China, and Russia based on non-extradition of former NSA contractor Edward Snowden after he released top secret information on U.S. cyber capabilities).

²⁹ See generally CLARKE & KNAKE, *supra* note 1, at 247-56 (discussing the value of an international agreement to ban certain kinds of cyber warfare activities and noting the hurdles that must be overcome in investigating attacks).

alone suggests that an international agreement is necessary.³⁰ “With companies and governments seemingly incapable of defending themselves from sophisticated cyber attacks and infiltration, there is almost universal belief that any durable cybersecurity solution must be transnational.”³¹ The Pentagon, for one, currently spends \$3.4 billion a year on developing cyber defensive and offensive capabilities.³² Of that, \$182 million is spent on U.S. Cyber Command, an organization led by the Pentagon,³³ staffing more than 13,000 employees.³⁴

China created its own cyber warfare unit in 2003,³⁵ with more than 250 groups of hackers in China alone capable of posing a threat to the United States.³⁶ A recent report from Mandiant, a U.S. cyber security company, argued that one group of China-based actors has hacked and compromised 141 companies across twenty major industries since 2006.³⁷ Mandiant argued that the group is actually a branch of the People’s Liberation Army of China.³⁸

Though attacks from China are most often cited in the news, Russia’s cyber capabilities far outmatch China’s and come closest to U.S. capabilities.³⁹ Through “a motley crew of government-sponsored cyber criminals and youth group members,” Russia “has integrated cyber operations into its military doctrine and is conducting strategic espionage against the United States.”⁴⁰ A 2010 Russian military doctrine called for “prior implementation of measures of modern information warfare in order to achieve

³⁰ See Adam Segal et al., *Why a Cybersecurity Treaty is a Pipe Dream*, COUNCIL ON FOREIGN RELATIONS (Oct. 27, 2011), <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>.

³¹ *Id.*

³² See SANGER, *supra* note 2, at 264.

³³ *Id.* at 263-64.

³⁴ *Id.* at 263.

³⁵ See CLARKE & KNAKE, *supra* note 1, at 57.

³⁶ *Id.* at 54.

³⁷ MANDIANT, APTI: EXPOSING ONE OF CHINA’S CYBER ESPIONAGE UNITS 3 (2013), available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

³⁸ *Id.*

³⁹ See CLARKE & KNAKE, *supra* note 1, at 63.

⁴⁰ See DAVID J. SMITH, RUSSIAN CYBER OPERATIONS 1 (July 2012).

political objectives without the utilization of military force.”⁴¹

Cyber units are also known to exist in Israel and France and are believed to exist in Taiwan, Iran, Australia, South Korea, India, and Pakistan, as well as in several NATO states.⁴² With such broad international exposure, it is only a matter of time before a relatively innocent cyber attack escalates to the point of open hostility or conflict.⁴³ Customary international law may stave off such a flashpoint, but an international cyber treaty might prove beneficial by providing more clarity on acceptable international norms.⁴⁴

B. Is Customary International Law Sufficient?

Most arguments against the creation of an international cyber treaty focus on whether customary international law precludes the need for a treaty.⁴⁵ For example, Heather Dinniss argues “[t]hose who call for a new convention have generally subscribed to the idea that cyberspace represents a fundamentally different conceptual space in which to fight. However, this approach . . . is simply not reflective of state practice in relation to other areas of internet law.”⁴⁶

The need for international agreement on specific details may already be precluded by customary international law. For instance, international law may sufficiently address what is necessary to claim self-defense against cyber attacks.⁴⁷ But a

⁴¹ See THE MILITARY DOCTRINE OF THE RUSSIAN FEDERATION: AN UNOFFICIAL TRANSCRIPT, available at <http://igcc.ucsd.edu/assets/001/502377.pdf>; see also SMITH, *supra* note 40, at 1.

⁴² See CLARKE & KNAKE, *supra* note 1, at 64.

⁴³ See generally *id.* at 64 (discussing how a series of cyber attacks could cripple United States infrastructure).

⁴⁴ See generally *id.* at 226-27 (discussing potential limitations on cyber war tactics).

⁴⁵ As noted below, customary international law creates a useful framework for analyzing cyber attacks. See *infra* Part III.B.

⁴⁶ See HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR 28 (2012).

⁴⁷ Sean Lawson, Op-Ed., *Cyberwarfare Treaty Would Be Premature, Unnecessary, and Ineffective*, U.S. NEWS AND WORLD REPORT (June 8, 2012), <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-treaty-would-be-premature-unnecessary-and-ineffective> (arguing that “existing international law is sufficient to determine when [cyber attacks] rise to the level of an ‘armed attack’ that justifies a military response”).

number of ambiguities still exist, the most basic of which is the lack of a universally accepted definition of what constitutes a cyber attack.⁴⁸ Dinniss notes as much in stating cyber attacks do not “fit neatly into the humanitarian law paradigm that has developed over the last century.”⁴⁹

C. What are the Benefits of an International Cyber Treaty?

A variety of practical arguments against a cyber treaty exist. For instance, a cyber treaty would likely limit the offensive and defensive options available to a state.⁵⁰ Military academies and think tanks alike might oppose the creation of a cyber treaty as “cyber weapons are inexpensive (compared to fighter jets, tanks, and aircraft carriers) and could reduce the overall level of force required to achieve an end goal.”⁵¹ Cyber tools also may not be sufficiently developed to merit the creation of a cyber treaty, especially as “such technologies are fundamentally dual use, widely available, and easy to conceal” making inspection and verification of such tools “virtually impossible.”⁵² This raises the serious concern that “a nation could move from a state of compliance to a gross violation in seconds and without warning.”⁵³

However, an international agreement would “make it more difficult for some kinds of cyber war attacks, while establishing norms of international behavior, providing international legal cover for nations to assist, and creating an international community of cooperating experts in fighting cyber war.”⁵⁴ For instance, a cyber treaty would be beneficial if it were to create a “no-first-use agreement.”⁵⁵ Such an agreement would not only have great diplomatic appeal but “might make it less likely that

⁴⁸ See *infra* Part III.A.

⁴⁹ See DINNISS, *supra* note 46, at 28.

⁵⁰ See Richard Stiennon, *Is an International Cyber Regulatory Agency Needed?*, FORBES CYBER DOMAIN BLOG (Aug. 22, 2012, 3:17 PM), <http://www.forbes.com/sites/richardstiennon/2012/08/22/is-an-international-cyber-regulatory-agency-needed/>.

⁵¹ *Id.*

⁵² See Lawson, *supra* note 47.

⁵³ See CLARKE & KNAKE, *supra* note 1, at 254.

⁵⁴ See *id.* at 253.

⁵⁵ See *id.* at 240 (“A no-first-use agreement could simply be a series of mutual declarations, or it could be a detailed international agreement. The focus could be on keeping cyber attacks from starting wars.”).

another nation would initiate cyber weapons use because to do so would violate an international norm that employing cyber weapons crosses a line, is escalatory, and potentially destabilizing.”⁵⁶

The nation that goes first and violates an agreement has added a degree of international opprobrium to its actions and created in the global community a presumption of misconduct. International support for that nation’s underlying position in the conflict might thus be undermined and the potential for international sanctions increased.⁵⁷

An international cyber treaty could also address the elusive concepts of attribution, self-defense, and enforcement.⁵⁸

III. Customary International Law and Cyber Warfare

If an international agreement is to be written, the first complication will be to define exactly what constitutes a cyber attack. Once cyber attack is defined, what customary international law applies and to what extent? Does a cyber attack constitute a threat or use of force as outlined by the U.N. Charter, and, if so, when does a cyber attack escalate to the point at which a nation can retaliate while claiming self-defense?

A. *The Need to Define*

No universally accepted definition of cyber attack exists. With terms such as “cyber attack,” “cyber espionage,” “cyber war,” and “cyber crime” often used interchangeably, several scholars have attempted to provide a specific yet comprehensive definition that could be used and agreed upon by the international community.⁵⁹ In doing so, they provide definitions that could guide international agreements and spark a dialogue on regulating cyber attacks.

In his book *Cyber War*, Richard Clarke defined “cyber warfare” as:

[T]he unauthorized penetration by, on behalf of, or in support of, a government into another nation’s computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or

⁵⁶ *See id.*

⁵⁷ *See id.*

⁵⁸ *See infra* Part IV.B-D.

⁵⁹ *See* CLARKE & KNAKE, *supra* note 1, at 227-28.

damage to a computer, or network device, or the objects a computer system controls.⁶⁰

Clarke's definition is criticized because it "limits the definition to attacks perpetrated by nation-states,"⁶¹ thus excluding non-state actors such as Anonymous or Al Qaeda.⁶² Clarke's definition also fails to distinguish cyber attacks from cyber crime or cyber war.⁶³

The Tallinn Manual⁶⁴ defines cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."⁶⁵ By emphasizing attack, this definition draws on Article 49(1) of Additional Protocol I which notes, "attacks means acts of violence against the adversary, whether in offence or defence."⁶⁶ Thus, cyber espionage and psychological cyber operations do not qualify as cyber attacks.⁶⁷ However, the manual curiously fails to define exactly what is meant by "cyber operation."⁶⁸ It is not, however, limited to attacks that result in kinetic effect.⁶⁹

The U.S. Department of Defense defines "computer network attack" as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."⁷⁰ "The defining feature of this form of attack is the

⁶⁰ See *id.* at 228.

⁶¹ Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 824 (2012).

⁶² See SANGER, *supra* note 2, at 265.

⁶³ See Hathaway et al., *supra* note 61, at 823.

⁶⁴ The Tallinn Manual is a manual written by an independent "International Group of Experts" which is meant to examine how legal norms influence cyber warfare. TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013) [hereinafter TALLINN MANUAL], available at http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381. The manual "results from an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare." *Id.* at 1.

⁶⁵ *Id.* at 106.

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ See TALLINN MANUAL, *supra* note 64, at 106.

⁷⁰ DOD DICTIONARY OF MILITARY TERMS, http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html (last visited Sept. 30, 2013).

fact that both the weapon and the target of the attack is the network itself and the information contained on such networks.”⁷¹ Thus, it is distinguished from non-computer based attacks such as an electro-magnetic pulse (EMP), radar, or radio attack.⁷² The definition also fails to cover attacks which would use computer networks to create kinetic effects elsewhere, such as on foreign nuclear centrifuges, as long as the information within the computers is not disrupted, denied, degraded, or destroyed.

Another recent definition focuses on the threat of cyber technologies, arguing, “[a] cyber attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.”⁷³ Therefore, the definition is not limited to a technology-based attack but is broad enough to incorporate kinetic attacks on computer infrastructure, such as the use of a regular explosive on undersea network cables.⁷⁴ The definition also focuses on the intent of the attack, distinguishing it from cyber crime,⁷⁵ and requires the attacked system be undermined, distinguishing it from cyber espionage.⁷⁶ But what if a cyber attack occurs for reasons other than politics or national security?

B. Customary International Law

As there is no universally accepted definition of cyber attack, there is also no universally accepted international law or agreement that governs cyber attacks. Instead, customary international law is used to address the initial threshold questions of “whether the existing law applies to cyber issues at all, and, if so, how.”⁷⁷ There is, however, a growing consensus among western legal scholars and nations that customary international law is applicable to cyber attacks.⁷⁸ President Obama voiced support

⁷¹ DINNISS, *supra* note 46, at 4.

⁷² *Id.* at 4.

⁷³ Hathaway et al., *supra* note 61, at 826.

⁷⁴ *Id.* at 827.

⁷⁵ *Id.* at 830.

⁷⁶ *Id.* at 828-30.

⁷⁷ See TALLINN MANUAL, *supra* note 64, at 3.

⁷⁸ See DINNISS, *supra* note 46, at 28; TALLINN MANUAL, *supra* note 64 at 3; Harold Koh, *International Law in Cyberspace*, U.S. DEP'T OF STATE, <http://www.state.gov/s/l/releases/remarks/197924.htm>; WHITE HOUSE STRATEGY, *supra* note 3, at 9. This note,

for this theory, stating, “[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete.”⁷⁹ Instead, the President claimed “[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.”⁸⁰

The commonly used framework for understanding cyber activities in international law focuses on distinguishing between cyber attacks covered by the law of war (*jus ad bellum*) and cyber attacks covered by law in war (*jus in bello*). *Jus ad bellum* encompasses law governing the lead-up to war, such as what constitutes a “use of force” in violation of Article 2(4) of the U.N. Charter.⁸¹ *Jus in bello* encompasses what types of cyber attacks would be allowed by customary international law once war has begun.⁸² Both influence what would be deemed appropriate attacks and responses to cyber attacks.

1. *Jus Ad Bellum*

For a cyber attack to constitute a prohibited act under customary international law, it must be shown that the attack rises to the level of a “threat or use of force” as provided by the U.N. Charter and that such force could be considered an “armed force.”⁸³ Generally, international law allows exceptions for collective security operations and actions taken in self-defense.⁸⁴ To date, no state has argued a cyber attack rises to the level of an armed attack or a prohibited use of force.⁸⁵

however, does not address legal theory from eastern legal scholars. Such scholarship is left to others to develop.

⁷⁹ WHITE HOUSE STRATEGY, *supra* note 3, at 9.

⁸⁰ *Id.* at 9.

⁸¹ See Schmitt, *supra* note 25, at 173 (“The *jus ad bellum* determines when a State has violated the international law governing the resort to force, and sets forth a normative flow plan for individually or collectively responding to such violations.”).

⁸² See *id.* at 173 (“By contrast, under the *jus in bello*, the applicability of IHL depends on the existence of an “armed conflict.”).

⁸³ DINNISS, *supra* note 46, at 40-41, 49.

⁸⁴ See Schmitt, *supra* note 25, at 160-62.

⁸⁵ See Hathaway et al., *supra* note 61, at 840.

i. The Use or Threat of Force

It is generally accepted as customary international law that states are prohibited from threatening or using force.⁸⁶ Article 2(4) of the U.N. Charter says all member states “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.”⁸⁷ Though the prohibition is “widely acknowledged as a cornerstone of both the United Nations Charter and of customary international law,” it is widely debated what exactly is meant by “force.”⁸⁸

Intense international debate centers on the precise scope of the concept of force.⁸⁹ The drafters of the U.N. Charter failed to define force, and neither the International Court of Justice nor the U.N. General Assembly has defined the term since.⁹⁰ A tension exists when one tries to remain faithful to the core values of the U.N. Charter while allowing sufficient flexibility to interpret constitutional norms.⁹¹ Thus, “[i]t appears that the ambiguity of the wording has been the price of international consensus.”⁹² Some states argue force should include both economic and political coercion.⁹³ However, it is generally accepted that force requires “armed force.”⁹⁴

Nations interpret “armed force” broadly.⁹⁵ Once force

⁸⁶ See Schmitt, *supra* note 25, at 153 (“Resultantly, it binds all States regardless of membership in the United Nations.”).

⁸⁷ U.N. Charter art. 2, para. 4.

⁸⁸ DINNISS, *supra* note 46, at 40.

⁸⁹ See Hathaway et al., *supra* note 61, at 842.

⁹⁰ See DINNISS, *supra* note 46, at 40.

⁹¹ *Id.* at 45.

⁹² *Id.* at 46.

⁹³ *Id.* at 41. “Weaker states and some scholars have argued that Article 2(4) broadly prohibits not only the use of armed force, but also political and economic coercion.” Hathaway et al., *supra* note 61, at 842.

⁹⁴ See DINNISS, *supra* note 46, at 41 (“Although no definitive conclusions have been drawn, the prevailing and commonly accepted view put forward by scholars is that the force referred to in Article 2(4) is limited to armed force.”).

⁹⁵ *Id.* at 49-50 (citing both *Corfu Channel (U.K. v. Alb.)*, 1949 I.C.J. 4, 13 and *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v U.S.)*, 1986 I.C.J. 14, 209 (June 27)).

comprises armed force, the question becomes whether a given cyber attack rises to the level of armed force. Michael Schmitt provides seven factors to consider when determining if an attack equates to a use of force: (1) severity of the damage, (2) immediacy of the consequences of the attack, (3) directness of the attack, (4) invasiveness of the act in the target state, (5) measurability of the damage, (6) presumptive legitimacy of the attack, and (7) the clarity of responsibility by a state for an attack.⁹⁶ These factors can be useful in determining whether a given cyber attack rises to the level of armed force.⁹⁷ Applying this framework, a cyber attack disabling a busy air traffic control system, resulting in plane crashes and subsequent death, would be considered a use of force, whereas the mere disruption of military-related research at a university via cyber attack would not be considered a use of force.⁹⁸

The International Court of Justice considers indirect acts of aggression as a use of force, though to a lesser degree.⁹⁹ This position by the court is especially salient as cyber attacks are often indirect acts or indirectly affect the target. For instance, a hacker might manipulate only a single, early step of a process, often allowing the hacker to mask the true origin of the attack, but still indirectly affecting the target.¹⁰⁰

ii. Exceptions to the Use or Threat of Force

The prohibition on the use of force within the U.N. Charter is subject to two exceptions: force is allowed in collective security actions taken by the U.N. Security Council and by state actions

⁹⁶ See Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914-15 (1998).

⁹⁷ *Id.* at 915 (“By this scheme, one measures the consequences of a computer network attack against the commonalities to ascertain whether they more closely approximate consequences of the sort characterizing armed force or whether they are better placed outside the use of force boundary.”).

⁹⁸ *Id.* at 916-17.

⁹⁹ See DINNISS, *supra* note 46, at 51.

¹⁰⁰ *Id.* at 65-67 (“Examples of such indirect attacks include a manipulation of GPS satellite systems to send an opposing force’s missiles off target, manipulation of hospital blood type data resulting in the wrong blood type being given to enemy soldiers, or disabling air traffic control systems.”).

taken in self-defense.¹⁰¹ Article 39 of the U.N. Charter provides “[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations or decide what measures shall be taken . . . to maintain or restore international peace and security.”¹⁰² Articles 41 and 42 allow the Security Council to determine whether to respond to “threat to the peace, breach of the peace, or act of aggression” with armed force.¹⁰³ However, any collective security operation requires approval from the “often deadlocked or slow-moving Security Council.”¹⁰⁴

Article 51 of the U.N. Charter provides an allowance for self-defense, noting “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs.”¹⁰⁵ In determining if self-defense is warranted and legitimate, the question becomes whether an armed attack preceded the claim of self-defense.¹⁰⁶ Thus, to legitimately claim self-defense and be allowed to use force in contravention of Article 2(4), a state must show it suffered from a cyber attack that rose to the level of an “armed attack.”¹⁰⁷ The concept of an armed attack is distinct from that of the use of force.¹⁰⁸ “Simply put, all armed attacks are uses of force, but not all uses of force qualify as armed attacks.”¹⁰⁹ Acts of self-defense are limited to uses of force that are necessary and proportional.¹¹⁰

¹⁰¹ See Hathaway et al., *supra* note 61, at 843.

¹⁰² U.N. Charter art. 39.

¹⁰³ See Schmitt, *supra* note 25, at 160-62.

¹⁰⁴ Hathaway et al., *supra* note 61, at 844.

¹⁰⁵ U.N. Charter art. 51.

¹⁰⁶ See Hathaway et al., *supra* note 61, at 844.

¹⁰⁷ See *id.* at 844.

¹⁰⁸ See Schmitt, *supra* note 25, at 163 (“In the *Nicaragua* case, the [International Court of Justice] acknowledged the existence of this gap between the notions of use of force and armed attack when it recognized that there are ‘measures which do not constitute an armed attack but may nevertheless involve a use of force’ and distinguished ‘the most grave forms of the use of force from other less grave forms.’”).

¹⁰⁹ See *id.* Notably, this is not the position of the U.S. government. See Koh, *supra* note 78.

¹¹⁰ See Schmitt, *supra* note 25, at 167.

2. *Jus in Bello*

Once an armed conflict has begun, the law of war, or *jus in bello*, applies.¹¹¹ Customary international law and the law of war are specifically implicated and complicated by cyber attacks in three ways: (1) the principle of distinction between combatants and civilians; (2) the proportionality of benefits of the attack in comparison to the unnecessary suffering of civilians; and (3) the concern for the neutrality of host states.¹¹²

i. Distinction

The principle of distinction “requires states to distinguish between civilian and military personnel and restrict attacks to military objectives.”¹¹³ As international law prohibits the targeting of civilian populations, states can use only weapons that are controllable, predictable, and can distinguish between military and non-military objectives.¹¹⁴ Attacks targeting civilian essentials such as food and water sources are prohibited.¹¹⁵

Kinetic warfare offers a much clearer application of the distinction principle, as the impact of conventional weapons is usually limited to a specific time and place.¹¹⁶ However, cyber attacks are unique in that “much of cyberspace is dual use—used by both the military and civilians.”¹¹⁷ Thus, “upholding the distinction requirement in cyberspace can be more challenging than it is in a conventional context.”¹¹⁸

Under *jus in bello*, “only three categories of individuals may be lawfully targeted: combatants, civilians directly participating in hostilities, and civilians acting in a continuous combat function.”¹¹⁹ The line between civilian and combatant is blurred when state-sponsored civilians use cyber attacks, such as Nashi, the “pro-Kremlin youth group started by Vladimir Putin,” which

¹¹¹ *See id.* at 173.

¹¹² *See* DINNISS, *supra* note 46, at 280.

¹¹³ Hathaway et al., *supra* note 61, at 851.

¹¹⁴ *See id.* at 852.

¹¹⁵ *See id.*

¹¹⁶ *See id.*

¹¹⁷ *See id.* at 852-53.

¹¹⁸ Hathaway et al., *supra* note 61, at 853.

¹¹⁹ *See id.* at 853.

took responsibility for the 2007 attacks on Estonia.¹²⁰ With the advent of botnets, the emergence of “hactivist” groups such as Anonymous, and the growing inability to accurately attribute responsibility for an attack to one actor, it is becoming increasingly clear that states walk a fine line when they seek to eliminate the cyber capabilities of an opposing state.

ii. Proportionality

The law of war requires the cancellation of any attack where the detrimental impact on civilians exceeds the military benefits.¹²¹ Specifically, Protocol I of the Geneva Conventions prohibits an attack that “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.”¹²² A proper proportionality analysis will consider the potential for civilian casualties, the destruction of civilian property, and the destruction of civilian items deemed indispensable against the potential benefit if the military objective is achieved.¹²³

Cyber attacks greatly complicate the proportionality analysis as the typical impact of a cyber attack is not measured in destruction of civilian property or indispensable items, but instead, often has indirect, nonlethal, or temporary effect.¹²⁴ For instance, it is unclear how to analyze the impact of eliminating access to a country’s banking system for a few days or of briefly erasing patient records at a nearby hospital.¹²⁵ Such temporary consequences “may force states to confront more uncertainty than they typically face in making decisions about the legality of planned attacks.”¹²⁶

¹²⁰ See *id.* at 854.

¹²¹ See *id.* at 850-51.

¹²² Geneva Protocol I Relating to the Protection of Victims of International Armed Conflicts, art. 57, ¶ 2b, *adopted on* June 8, 1977, *available at* <http://treaties.un.org/untc//pages//doc/Publication/UNTS/volume%201125/volume-1125-I-17513-English.pdf>.

¹²³ See Hathaway et al., *supra* note 61, at 850-51.

¹²⁴ See *id.* at 851.

¹²⁵ See *id.*

¹²⁶ See *id.*

iii. Neutrality

Neutrality is another issue complicated by cyber attacks.¹²⁷ The primary benefit of neutrality to a state is inviolability—the duty of belligerent states to respect the rights of the neutral.¹²⁸ To maintain this benefit, a state is required to remain impartial and abstain from any actions to the contrary.¹²⁹ Only then can the neutral state insist upon its own inviolability.¹³⁰ However, complications arise when the facilities of a neutral power, for example, the communications infrastructure of Switzerland, are used to conduct a cyber attack against another state.¹³¹ Scholars differ on whether it is the responsibility of the neutral power to block the use of its facilities or whether it need only abstain from helping to build such facilities.¹³²

IV. Cyber Treaty Bare Bones

To fully consider whether the international community should pursue a cyber treaty, it is useful to illustrate exactly what an international cyber agreement could look like. Applying customary international law to cyber attacks creates a number of ambiguities that an international agreement would help to clarify.¹³³ In particular, the international community would benefit from a clear definition of cyber attack, as well as clarification on the critical issues of attribution, self-defense, and enforcement.

A. Initial Concerns for a Definition

States will be hard pressed to coordinate any real multi-national defense and response mechanisms without a common definition of cyber attack.¹³⁴ Any international agreement will necessarily define cyber attack and in doing so will establish the scope and potential benefit of the agreement.¹³⁵ If the definition is

¹²⁷ See *id.* at 855.

¹²⁸ See *id.*

¹²⁹ See Hathaway et al., *supra* note 61, at 855

¹³⁰ See *id.*

¹³¹ See *id.*

¹³² See *id.*

¹³³ See *id.* at 877.

¹³⁴ See *id.*

¹³⁵ See Hathaway et al., *supra* note 61, at 880-81.

too broad, such as by including cyber crime or cyber espionage, the agreement will not be easily verifiable or enforceable.¹³⁶ However, a broad definition may be the only realistic option as “consensus may only be reached by allowing for differing interpretations.”¹³⁷

The debate currently splitting states is whether to adopt a means-based or effects-based approach to defining cyber attack.¹³⁸ The means-based approach defines cyber attacks by the *methods* in which they are conducted, for example through new information and communication technologies.¹³⁹ The effects-based approach defines cyber attacks by the *objective* of an attack, for instance “shaping the behaviour of friends, foes and neutrals in peace, crisis, and war.”¹⁴⁰ The impact of non-state actors complicates any definition of cyber attack, as does the need to consider whether a kinetic effect is necessary or if the mere altering of information is sufficient.¹⁴¹

B. Attribution: State and Non-State Actors

One vital component of any cyber treaty will be to determine and define the evidence necessary to prove a particular cyber attack is attributable to a specific state or non-state actor. Attribution is critical to legitimate claims of self-defense.¹⁴² For long-term responses, attribution is necessary to support reparation claims.¹⁴³ As noted by Harold Koh while serving as Legal Adviser to the U.S. State Department, “cyberspace significantly increases an actor’s ability to engage in attacks with ‘plausible deniability,’ by acting through proxies.”¹⁴⁴ Thus, without sufficient clarity on the elements needed to prove attribution, a treaty would be wholly ineffective as a state could easily hide behind proxies from

¹³⁶ See CLARKE & KNAKE, *supra* note 1, at 254.

¹³⁷ See DINNISS, *supra* note 46, at 9.

¹³⁸ See Hathaway et al., *supra* note 61, at 824-25.

¹³⁹ See *id.* at 825.

¹⁴⁰ See DINNISS, *supra* note 46, at 24.

¹⁴¹ See Koh, *supra* note 78.

¹⁴² See *infra* Part IV.C.

¹⁴³ See *infra* Part IV.D.

¹⁴⁴ Koh, *supra* note 78.

sanctions and other potential remedies.¹⁴⁵

1. *State Actors*

When a government agent acts, even if such acts are not authorized, the state is legally responsible for the effect of the acts.¹⁴⁶ A state agent includes “all the individual or collective entities which make up the organization of the State and act on its behalf.”¹⁴⁷ Thus, any cyber attack conducted by agents of the state that constitutes an unlawful use of force will infer responsibility on the state.¹⁴⁸

While it may seem fairly straightforward that a state is held responsible for the action of its agents, the difficulty lies in the subtle nature of cyber attacks. For instance, cyber attack technologies are not as readily detectable as chemical or nuclear weapons.¹⁴⁹ Instead, “a nation [can] hide its cyber weapons on thumb drives or CDs anywhere in the country.”¹⁵⁰ Perhaps for this reason, to date, no cyber attack has been conclusively attributed to a state.¹⁵¹ This, in part, is why a universally accepted definition of cyber attack is necessary. However, a cyber treaty should go beyond defining cyber attack to explicitly detail what evidence is needed to attribute a cyber attack to a state or its agents.¹⁵² Without such clarity, states will continue to successfully hide behind proxies.¹⁵³ The international community should also address how neutral states are implicated when agents of one state use the networks of a neutral state.

2. *Non-state Actors*

The issue of attribution for non-state actors is considerably

¹⁴⁵ *See id.*

¹⁴⁶ Report of the International Law Commission, Draft Articles on Responsibility of States for International Wrongful Acts, 53rd Sess., Apr. 23-June 1, July 2-Aug.10, art. 4, U.N. Doc. A/56/10 (2008) [hereinafter Draft Articles] available at http://legal.un.org/ilc/texts/instruments/english/draftarticles/9_6_2001.pdf.

¹⁴⁷ *Id.* art. 4, cmt. 1.

¹⁴⁸ Schmitt, *supra* note 25, at 157.

¹⁴⁹ *See* CLARKE & KNAKE, *supra* note 1, at 247-48.

¹⁵⁰ *See id.* at 248.

¹⁵¹ *See* DINNISS, *supra* note 46, at 53.

¹⁵² *See* Hathaway et. al., *supra* note 61, 877.

¹⁵³ *See* Koh, *supra* note 78.

more complicated than that of state actors. Non-state actors cannot violate the customary international law norm against the use of force substantiated by Article 2(4) of the U.N. Charter unless there can be shown a clear relationship with a state.¹⁵⁴ When an action can be attributed to the state and it constitutes a breach of an international obligation, it is considered an internationally wrongful act.¹⁵⁵ Thus, to incorporate the actions of non-state actors, an international cyber treaty should identify when a non-state actor is deemed to have a clear relationship with a state.¹⁵⁶ For instance, Michael Schmitt argued that without clear evidence of Russian governmental involvement in the 2007 cyber attacks on Estonia, “none of those individuals or groups conducting the operations violated the Article 2(4) prohibition.”¹⁵⁷ Instead, he argued, the non-binding law of state responsibility governs.¹⁵⁸

The law of state responsibility asserts that conduct directed or controlled by a state “shall be considered an act of a State . . . if the person or group of persons is in fact acting on the *instructions* of, or under the *direction* or *control* of, that State in carrying out the conduct.”¹⁵⁹ There must be “a specific factual relationship” between the non-state actor and the state for the actions to be attributable to the state.¹⁶⁰ Such a relationship may exist “where State organs supplement their own action by recruiting or instigating private persons or groups who act as ‘auxiliaries’ while remaining outside the official structure of the State.”¹⁶¹ Thus, “attribution requires (1) acts qualifying as an armed attack and (2) that the State dispatched the non-state actors or was substantially involved in the operations.”¹⁶²

¹⁵⁴ Schmitt, *supra* note 25, at 157.

¹⁵⁵ See Draft Articles, *supra* note 146, art. 2.

¹⁵⁶ See Schmitt, *supra* note 25, at 157.

¹⁵⁷ See *id.*

¹⁵⁸ See *id.*

¹⁵⁹ Draft Articles, *supra* note 146, at 47-48 (emphasis added) (“[T]he three terms ‘instructions,’ ‘direction’ and ‘control’ are disjunctive; it is sufficient to establish any one of them.”).

¹⁶⁰ *Id.* at 47.

¹⁶¹ *Id.*

¹⁶² Schmitt, *supra* note 25, at 171 (noting, however, that the standard may have been relaxed in the aftermath of the 9/11 attacks where the Al Qaeda attack was

However, the law on state responsibility does not address actions of non-state actors acting outside the purview of a state,¹⁶³ for instance terrorist organizations like Al Qaeda¹⁶⁴ or activist collectives such as Anonymous.¹⁶⁵ An international cyber treaty could be critical in filling this gap.¹⁶⁶ A treaty could “shift the burden of stopping [such cyber attacks] to the states party to the convention.”¹⁶⁷ Such a treaty provision would take advantage of the international norm that a state may be held responsible for the acts of non-state actors that occur within the state when the state “fails to take reasonably available measures to stop such acts in breach of its obligations to other States.”¹⁶⁸

The “arsonist principle” mirrors such an approach.¹⁶⁹ The principle is based on the notion that the community will hold an individual responsible for the actions of an arsonist if the individual knowingly harbors the arsonist.¹⁷⁰ While cyber attacks often occur outside of the physical world, such attacks are “made

attributed to the Taliban in Afghanistan even though there was no clear showing of substantial involvement, instead finding sufficient involvement where the Taliban “merely provided sanctuary”).

¹⁶³ See Draft Articles, *supra* note 146, at 34 (noting specifically these articles “deal only with the responsibility of States”).

¹⁶⁴ See Schmitt, *supra* note 25, at 171 (“Al Qaeda computers have been seized that contain hacker tools, the membership of such groups is increasingly computer-literate, and the technology to conduct cyber operations is readily available.”).

¹⁶⁵ See Alister Bull & Jim Finkle, *Fed Says Internal Site Breached by Hackers, No Critical Functions Affected*, REUTERS (Feb. 6, 2013, 9:30 AM), <http://www.reuters.com/article/2013/02/06/net-us-usa-fed-hackers-idUSBRE91501920130206> (reporting a cyber attack by Anonymous on the U.S. Federal Reserve resulted in the infiltration of an emergency communications system used by banks during natural disasters).

¹⁶⁶ See Schmitt, *supra* note 25, at 173 (noting although Article 51 of the U.N. Charter and the customary law of self-defense have been traditionally applicable solely to armed attacks by one State against another, violent actions by non-State actors, such as the 9/11 attacks by Al Qaeda, have been nonetheless treated under the law of self-defense).

¹⁶⁷ CLARKE & KNAKE, *supra* note 1, at 270 (“Nations would be required to rigorously monitor for hacking originating in their country and to prevent hacking activity from inside their territory.”).

¹⁶⁸ See Schmitt, *supra* note 25, at 158.

¹⁶⁹ See CLARKE & KNAKE, *supra* note 1, at 249.

¹⁷⁰ See *id.* (“If you have an arsonist in your basement; and every night he goes out and burns down a neighbor’s house, and you know this is going on, then you can’t claim you aren’t responsible.”).

up of physical components” located in sovereign nations.¹⁷¹ “Even if the attacker could not be identified, at least there would be someone who could be held responsible for stopping the attack and investigating who the attacker was.”¹⁷² Application of the principle “would make each person, company, ISP, and country responsible for the security of their piece of cyberspace.”¹⁷³ Taking the thought a step further, a state with such an “arsonist” in its midst should not only be held responsible for police-like activities, but should also have an “obligation to assist” under an international cyber agreement.¹⁷⁴ The responsible state could then be required “to respond quickly to inquiries in international investigations, seize and preserve server or router records, host and facilitate international investigators, produce their citizens for questioning, and prosecute citizens for specified crimes.”¹⁷⁵

The Tallinn Manual offers one such rule, noting “[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.”¹⁷⁶ The Manual notes this rule “applies irrespective of the attributability of the acts in question to a State.”¹⁷⁷ Thus, it would not matter whether the state were involved in or responsible for the cyber attack; the state would be held responsible even if it were merely a sanctuary for illegal cyber attacks against other states.¹⁷⁸

C. Responding to Cyber Attacks: U.N. Security Council, Self Defense, and Countermeasures

Response to a cyber attack initiated during a war must comply with customary international law principles, including those of

¹⁷¹ See *id.* (referring to physical components “from the high-speed fiber-optic trunks, to every router, server, and ‘telecom hotel’ . . . except perhaps for the undersea cables and the space-based relays”).

¹⁷² *Id.* at 251.

¹⁷³ *Id.* at 249.

¹⁷⁴ *Id.* at 250.

¹⁷⁵ CLARKE & KNAKE, *supra* note 1, at 250.

¹⁷⁶ See TALLINN MANUAL, *supra* note 64, at 26.

¹⁷⁷ *Id.* at 26.

¹⁷⁸ See, e.g., Schmitt, *supra* note 25, at 171 (noting that the Al Qaeda attack was attributed to the Taliban in Afghanistan when the Taliban “merely provided sanctuary”).

distinction, proportionality, and neutrality.¹⁷⁹ More relevant to current conditions is the appropriate response to cyber attacks that occur *jus ad bellum*, or prior to the initiation of war. Under customary international law, there are two exceptions to the prohibition on the use of force:¹⁸⁰ (1) the U.N. Security Council can choose to use force when a particular incident amounts to a “threat to the peace, breach of the peace, or act of aggression;”¹⁸¹ and (2) a Member of the United Nations may use force in self-defense in response to an armed attack.¹⁸²

A cyber treaty might provide little benefit to the first exception, as the “often deadlocked” Security Council must determine when collective action is appropriate¹⁸³ and is subject to the veto right of the five Permanent Members of the Security Council.¹⁸⁴ However, since the most immediate tool for a state to respond to cyber attacks might be the authority to use force in self-defense, a cyber treaty could benefit the international community by clarifying what is necessary for a cyber attack to constitute an armed attack.¹⁸⁵ In determining if a cyber attack has risen to the level of an armed attack, three competing views have emerged: the instrument-based approach, the target-based approach, and the effects-based approach.¹⁸⁶ The instrument-based approach focuses on the tools used in an attack, arguing that to be an armed attack the attacker must use traditional military weapons.¹⁸⁷ The target-based approach focuses on what is targeted, thus meriting self-defense when the target is “a sufficiently important computer system.”¹⁸⁸ The effects-based approach focuses on the overall impact of the attack, thus meriting self-defense when the attack is

¹⁷⁹ See *supra* Part III.B.

¹⁸⁰ See Schmitt, *supra* note 25, at 160-62.

¹⁸¹ See U.N. Charter arts. 39, 41 & 42.

¹⁸² *Id.* art. 51.

¹⁸³ See Hathaway et al., *supra* note 61, at 844.

¹⁸⁴ See Schmitt, *supra* note 25, at 162.

¹⁸⁵ See *generally id.* at 163-64 (noting that while existing law suggests that “armed attack” typically requires kinetic force, the potentially devastating consequences of non-kinetic cyber attacks make the current interpretation “wholly unsatisfactory”).

¹⁸⁶ See Hathaway et al., *supra* note 61, at 845.

¹⁸⁷ See *id.* at 845-46.

¹⁸⁸ *Id.* at 846-47 (“A cyber-attack need only penetrate a critical system to justify a conventional military response that could start a physical, kinetic war.”).

of sufficient gravity.¹⁸⁹

The self-defense component of Article 51 of the U.N. Charter was drafted with an instrument-based approach in mind.¹⁹⁰ Michael Schmitt argues this choice by the drafters of the U.N. Charter to use an instrument-based approach is inappropriate for addressing self-defense claims against cyber attacks.¹⁹¹ Because armed attacks inherently include kinetic military force,¹⁹² and because cyber attacks often utilize non-kinetic approaches, the instrument-based approach fails to encapsulate cyber attacks that do not look like armed attacks but have the same ultimate effect.¹⁹³ Instead, he argues an effects-based approach, though not the current norm of international law, would better address cyber attacks because it allows broader latitude for a state to respond in self-defense.¹⁹⁴

Ultimately, a cyber treaty would benefit the international community by deciding if and when a cyber attack constitutes an armed attack, thus determining when claims of self-defense and subsequent uses of force would be legitimate.¹⁹⁵ The U.S. has unilaterally moved in this direction, arguing “[c]onsistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace.”¹⁹⁶ Whether other states agree and to what extent would be critical considerations for a cyber treaty.

When responding to international law violations that do not rise to the level of an armed attack, an injured state may sometimes use “countermeasures” even if the initial use of force

¹⁸⁹ See *id.* at 847; see also DINNISS, *supra* note 46, at 113 (“Classification of computer network attacks which would amount to armed attacks should therefore be restricted to those attacks which cause physical damage to property or persons of a sufficient scale and effect.”).

¹⁹⁰ See Schmitt, *supra* note 25, at 163.

¹⁹¹ *Id.*

¹⁹² See *id.* (“Clearly, an armed attack includes kinetic military force.”).

¹⁹³ Schmitt, *supra* note 25, at 163-64.

¹⁹⁴ *Id.*

¹⁹⁵ Hathaway et al., *supra* note 61, at 881-82 (noting that while developing a shared definition of cyber attack could lead to more extensive international cooperation, an agreement that would be limited to a common definition would likely face challenges).

¹⁹⁶ WHITE HOUSE STRATEGY, *supra* note 3, at 10.

does not rise to the level of an armed attack.¹⁹⁷ Countermeasures are “measures that would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.”¹⁹⁸ Countermeasures may be used in response to an ongoing wrong; however, they must be proportionate to the injury suffered, and the victim-state must first ask the injuring State to end the wrong.¹⁹⁹ Countermeasures are a less effective tool against cyber attacks than self-defense for the victim-state because countermeasures do not legitimize the threat or use of force.²⁰⁰ In drafting a cyber treaty, the international community could benefit from countermeasures if the cyber attack definition is limited to something less than an armed attack.²⁰¹

D. Enforcement: Reparations and Compliance

Ensuring enforcement of an international cyber treaty is complicated by the nature of cyber attacks as well as the lack of a clear definition. The law of state responsibility, codified in 2001 by the International Law Commission,²⁰² provides the basic framework for understanding state obligations and remedies for cyber attack. If a state is found to be responsible for an illegal international act, it is “under an obligation to make full reparation for the injury caused.”²⁰³ Reparation can include restitution, compensation, or satisfaction.²⁰⁴ Restitution is an obligation to “re-establish the situation which existed before the wrongful act

¹⁹⁷ Hathaway et al., *supra* note 61, at 857; *see also* Draft Articles, *supra* note 146, at 128 (explaining that countermeasures are in response to “retorsion” or unfriendly conduct, while reprisals are in response to international armed conflict).

¹⁹⁸ Draft Articles, *supra* note 146, at 128.

¹⁹⁹ *See* Schmitt, *supra* note 25, at 159-60.

²⁰⁰ *See id.* at 160 (“Responses amounting to a use of force are only permissible when falling within the two recognized exceptions to the prohibition on the use of force—action authorized by the Security Council and self-defense.”).

²⁰¹ *See* Hathaway et al., *supra* note 61, at 857.

²⁰² *See* Draft Articles, *supra* note 146, cover.

²⁰³ *Id.*, *supra* note 146, art. 31, ¶ 1; *see also id.* art. 31, ¶ 2 (“Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State.”).

²⁰⁴ *Id.* art. 34; *see also* Schmitt, *supra* note 25, at 159.

was committed” as long as it is not materially impossible or overly burdensome to do so.²⁰⁵ Compensation includes repayment of “any financially assessable damage” caused by the wrongful act.²⁰⁶ Satisfaction is an obligation that exists where restitution or compensation are unable to make whole the victim-state and can include, *inter alia*, acknowledgment of the wrong caused, expression of regret, or a formal apology.²⁰⁷

While the law of state responsibilities provides initial answers as to what a responsible state might be asked to do, true enforcement must also include compliance. Under customary international law, the U.N. stands as the enforcer of international laws.²⁰⁸ However, in terms of cyber attacks, the U.N. will undoubtedly need to rely upon member states to enforce any reparations.²⁰⁹

Clarke argues “[t]o judge whether a nation is actively complying or is just being passive-aggressive, it may be useful if a cyber war agreement created an ‘International Cyber Forensics and Compliance Staff.’”²¹⁰ According to Clarke, a staff of experts would be used to report on compliance with the international agreement, including an international inspection team similar to those used for nuclear nonproliferation agreements.²¹¹ “Nations that were found to be scofflaws could be subject to a range of sanctions.”²¹² Still, he notes, “high-confidence verification of compliance with a cyber war limitation agreement will not be possible.”²¹³

V. Is an International Cyber Treaty Feasible?

Even though a cyber treaty would clarify ambiguities in

²⁰⁵ Draft Articles, *supra* note 146, art. 35.

²⁰⁶ *Id.* art. 36, ¶ 2.

²⁰⁷ *Id.* art. 37, ¶¶ 1-2.

²⁰⁸ *See* Schmitt, *supra* note 25, at 162.

²⁰⁹ *See id.* (“Since the United Nations does not itself control cyber networks or have the capability to mount cyber operations, it would have to rely on States to effectuate any cyber related resolutions.”).

²¹⁰ *See* CLARKE & KNAKE, *supra* note 1, at 252.

²¹¹ *See id.*

²¹² *Id.* at 253.

²¹³ *Id.* at 254.

applying international law to cyber attacks, perhaps the more relevant question is whether an agreement can exist in the first place. Members of the international community will need to agree to move forward. The diverse and often conflicting interests of each state, as well as the varied technological capabilities, will need to be considered and sufficiently addressed.

A. *Conflicting International Interests and Technology Dependence*

The main players on the international stage concerning cyber attacks are the U.S., China, and Russia.²¹⁴ The interests of these and other technologically-advanced states differ based on “different strategic priorities, internal politics, public-private relationships, and vulnerabilities” which “will continue to pull them apart on how cyberspace should be used, regulated, and secured.”²¹⁵ Still, technologically advanced also means technologically dependent, a lesson all too clear to U.S. leaders.²¹⁶ It may very well be this technological dependence that forces an agreement as dependence inevitably leads to vulnerability in one’s defenses.

1. *Identifying Interests of the Key Players*

Lines are being drawn between western states, including the U.S. and other NATO states, and eastern states, including Russia and China.²¹⁷ “While the United States, the United Kingdom and their like-minded allies emphasize the protection of computer networks from damage and theft, Russia, China and their partners emphasize information security, which to them means controlling content and communication or social networking tools that may threaten regime stability.”²¹⁸ With Russia and China the other

²¹⁴ See *supra* Part II.A.

²¹⁵ See Segal, *supra* note 30. For instance, at least five countries have declared that Internet access is a fundamental human right. See DINNISS, *supra* note 46, at 11 n.35 (including Costa Rica, Estonia, Finland, France, and Greece).

²¹⁶ See CLARKE & KNAKE, *supra* note 1, at 145 (quoting former U.S. Vice Admiral John Michael McConnell as stating that “[b]ecause [the U.S. is] the most developed technologically—we have the most bandwidth running through our society and are more dependent on that bandwidth—we are the most vulnerable”).

²¹⁷ See Segal, *supra* note 30.

²¹⁸ See *id.* (stating in preparation for a 2011 conference in London on cyber

major players in the cyber game, the U.S. will need to contemplate its interests to put together a comprehensive cyber treaty.²¹⁹

Russia shows little recent interest in negotiating an international cyber treaty,²²⁰ though a Russian proposal was rejected during the Clinton administration.²²¹ Notably, Russia's goals for information security differ from most other states,²²² focusing on "the spiritual renewal of Russia" and "information support for the state policy of the Russian Federation."²²³ For instance, Russia's government "considers the 'information war,' conducted by the press for public opinion, to be a very important aspect of keeping the emotions and loyalties of its people in check during crisis."²²⁴ In light of the recent cooling of relations between the United States and Russia, in no small part due to Russia's decision to grant asylum to former NSA contractor Edward Snowden²²⁵ and the tensions brought on by the competing positions on Syria's chemical weapons,²²⁶ it is becoming increasingly less likely that the two states would have interest in negotiating a cyber treaty. The choice by the White House to

security, "representatives of China, Russia, Tajikistan, and Uzbekistan proposed to the U.N. Secretary-General an International Code of Conduct for Information Security, which addresses cyber security but also calls on states to curb the dissemination of information which 'undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.").

²¹⁹ See *id.*

²²⁰ See SMITH, *supra* note 40, at 1 ("[Russia] spares no diplomatic effort in trying to forge a path forward for its nefarious activities while resisting efforts to do anything constructive in the international arena.").

²²¹ See CLARKE & KNAKE, *supra* note 1, at 219.

²²² See SMITH, *supra* note 40, at 2-3.

²²³ See *Information Security Doctrine of the Russian Federation*, MINISTRY FOREIGN AFFAIRS RUSSIAN FEDERATION (Sept. 9, 2000), <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument>.

²²⁴ See Timothy L. Thomas, *Nation-state Cyber Strategies: Examples from China and Russia*, in CYBERPOWER AND NATIONAL SECURITY 465, 484 (Franklin D. Kramer et al. eds., 2009).

²²⁵ Paul Sonne & Adam Entous, *Snowden Asylum Hits U.S.-Russia Relations*, WALL ST. J., Aug. 1, 2013, <http://online.wsj.com/article/SB10001424127887323681904578641610474568782.html>.

²²⁶ See Larisa Epatko, *Despite Snowden and Syria Cooling U.S.-Russian Relations, Work Goes On*, PBS (Sept. 5, 2013), available at <http://www.pbs.org/newshour/rundown/2013/09/us-russia.html>.

cancel a Russian summit for the first time in decades complicates things further.²²⁷ Any viable cyber treaty will need agreement or at least mutual respect from the two states.

Whereas Russian interest in cyber focuses more on boosting Russia's international prestige and protecting the state,²²⁸ Chinese interests in cyber attacks appear to be in raiding corporate and defense secrets.²²⁹ To this end, Chinese advancements in cyber attacks "ha[ve] been, oddly, somewhat transparent."²³⁰ U.S. companies including Apple, Twitter, and Facebook, as well as news organizations including The New York Times, The Wall Street Journal, and The Washington Post have been the victims of cyber attacks considered to have originated in China.²³¹ Notably, the U.S. tried "in 2010 and 2011[] to have some quiet conversations with the Chinese about cyberweaponry and limits on their use."²³²

2. *Technological Dependence*

The true driver for a cyber treaty may be fear of the rogue Third World state or non-state actor interested in using cyber attacks to disrupt the economies and critical infrastructure of the first world. Cyber attacks "are a product of, and are the greatest threat to, those societies which place a high value on information."²³³ As technological dependence increases within a

²²⁷ Peter Baker & Steven Lee Myers, *Ties Fraying, Obama Drops Putin Meeting*, N.Y. TIMES, Aug. 7, 2013, http://www.nytimes.com/2013/08/08/world/europe/obama-cancels-visit-to-putin-as-snowden-adds-to-tensions.html?ref=politics&_r=0.

²²⁸ See *Information Security Doctrine of the Russian Federation*, *supra* note 223.

²²⁹ See, e.g., SANGER, *supra* note 2, at 263 ("[A] second, less discussed element of the [Chinese cyber] attack also stole source code—the heart of Google's business."); see also CLARKE & KNAKE, *supra* note 1, at 233 ("In April 2009, someone broke into data storage systems and downloaded terabytes' worth of information related to the development of the F-35. . . . With a high degree of certainty, [Pentagon officials] believe that the intrusion can be traced back to an IP address in China . . . that . . . implicates Chinese government involvement.").

²³⁰ See, e.g., CLARKE & KNAKE, *supra* note 1, at 233.

²³¹ See HEATHER KELLY, *Apple: We were hacked, too*, CNN, http://www.cnn.com/2013/02/19/tech/web/apple-hacked/index.html?hpt=hp_t2 (last updated Feb. 19, 2013, 7:24 PM).

²³² See SANGER, *supra* note 2, at 265.

²³³ See DINNISS, *supra* note 46, at 33.

state, vulnerability to cyber attacks also increases.²³⁴ For instance, non-state actors and less technologically advanced states can have an asymmetric advantage on technologically advanced states such as the U.S. because they are less dependent on cyber technologies.²³⁵

Unlike the development of nuclear bombs, cyber weapons are cheap and easily created.²³⁶ They are not just the playthings of superpowers but are easily available to all who seek them.²³⁷ Thus, “cyber-attacks may prove to be a powerful weapon of the weak.”²³⁸ Fear of such power may spur the current superpowers to impose a cyber treaty on their brethren to ensure that technology dependence does not become a crutch.²³⁹

B. Agreement to Move Forward

With the potential dramatic impact of cyber attacks on the international community—especially the most technologically advanced nations²⁴⁰—states are beginning to come together to address potential cyber threats. In July of 2010, a U.N. panel of cyber-security specialists from fifteen countries, including the U.S., China, and Russia, submitted recommendations on an international framework for security and stability in new technologies.²⁴¹ The panel made five recommendations: (1) further international dialogue to discuss norms; (2) engage in measures to build confidence and stability and to reduce risk; (3) engage in information exchanges on national legislation and security strategies, technologies, policies, and best practices; (4) identify measures to build capacity for less developed countries;

²³⁴ See CLARKE & KNAKE, *supra* note 1, at 145.

²³⁵ See, e.g., *id.* at 149 (noting that “North Korea has so few systems dependent upon cyberspace that a major cyber war attack on North Korea would cause almost no damage”).

²³⁶ See Hathaway et al., *supra* note 61, at 842.

²³⁷ See *id.*

²³⁸ *Id.*

²³⁹ See *id.*

²⁴⁰ See DINNISS, *supra* note 46, at 1.

²⁴¹ U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, U.N. Doc. A/65/201 (July 30, 2010).

and (5) find ways to elaborate on common terms and definitions.²⁴²

States can move forward unilaterally, bilaterally, or multilaterally, through the distribution of joint declarations, communication of redlines, or international agreements.²⁴³ Arguments are being made that the U.S. “should issue substantive statements about thresholds and response” effectively providing a unilateral statement with a goal “to spur others to issue similar commitments.”²⁴⁴ The White House has effectively done this through the publication of the International Strategy for Cyberspace, stating “[t]he United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnership.”²⁴⁵ The White House contends “[w]e will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace.”²⁴⁶ Harold Koh noted, “[W]e are actively engaged with the rest of the international community, both bilaterally and multilaterally, on the subject of applying international law in cyberspace.”²⁴⁷ The U.N., including several of the major players in the Security Council, has already taken the first steps toward constructing an international understanding of cyber attacks.²⁴⁸ Notably, many of the most interested parties are major first-world actors that are highly dependent on technology.²⁴⁹

Ultimately, fear of the asymmetrical advantage maintained by states without technological dependence may bring leading states such as the U.S., China, and Russia to the negotiation table. Those providing the best technological incentives may seek to sway

²⁴² See *id.* at 8.

²⁴³ See Segal, *supra* note 30.

²⁴⁴ ADAM SEGAL & MAURICE R. GREENBERG, CYBERSPACE GOVERNANCE: THE NEXT STEP 3 (2011), available at <http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397>.

²⁴⁵ WHITE HOUSE STRATEGY, *supra* note 3, at 9 (stating that “we will work to build a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these systems as essential to the national and collective interest”).

²⁴⁶ See *id.* at 9.

²⁴⁷ Koh, *supra* note 78.

²⁴⁸ See DINNISS, *supra* note 46, at 27.

²⁴⁹ See *id.* at 33.

weaker states.²⁵⁰ “Cyber security expertise is lacking in Latin America, Africa and Southeast Asia and governments will turn to whoever can provide it.”²⁵¹ This may lead stronger states to argue for more expansive readings of the self-defense and use of force articles in the U.N. Charter, allowing states greater latitude when responding to cyber attacks.²⁵²

The U.S. may be moving toward the negotiation table. In a major speech at U.S. Cyber Command, Harold Koh said, “[b]ut to those who say that established law is not up to the task, we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed.”²⁵³ He argued “[d]eveloping common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area.”²⁵⁴

VI. Conclusion

This note provided the framework for movement toward an international cyber treaty by demonstrating how a cyber treaty would be of use, outlining relevant customary international law, illustrating the ambiguities created when such law is applied to cyber attacks, and beginning the assessment of the feasibility of such a treaty. As Richard Stiennon explains, “This debate is going to rage for quite a while. There will be no short term resolution and we will see an escalating arms race and cyber weapons incorporated in most arsenals long before we see any international agreement to restrict cyber arms.”²⁵⁵

We can play the role of realist, accepting the world as we see it and trying to solve the problems before us—or a more critical approach is possible, asking how things came to be and seeking a “transformative structural change.”²⁵⁶ Both approaches will

²⁵⁰ See Segal, *supra* note 30.

²⁵¹ See *id.*

²⁵² See Hathaway et al., *supra* note 61, at 842.

²⁵³ Koh, *supra* note 78.

²⁵⁴ *Id.*

²⁵⁵ Richard Stiennon, *Is an International Cyber Regulatory Agency Needed?*, FORBES CYBER DOMAIN BLOG (Aug. 22, 2012, 3:17 PM), <http://www.forbes.com/sites/richardstiennon/2012/08/22/is-an-international-cyber-regulatory-agency-needed/>.

²⁵⁶ See ABIGAIL E. RUANE & PATRICK JAMES, *THE INTERNATIONAL RELATIONS OF MIDDLE-EARTH: LEARNING FROM THE LORD OF THE RINGS* 35 (2012).

2013

INTERNATIONAL CYBER TREATY

257

undoubtedly play a role in devising a comprehensive cyber treaty. This is the first step in that direction.