EMORY LAW

Emory International Law Review

Volume 26 | Issue 2

2012

State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights

Catherine Lotrionte

STATE SOVEREIGNTY AND SELF-DEFENSE IN CYBERSPACE: A NORMATIVE FRAMEWORK FOR BALANCING LEGAL RIGHTS

Catherine Lotrionte[*]

> Today's threats recognize no national boundaries, are connected, and must be addressed at the global and regional as well as the national levels.[1]

> When warranted, [the United States] will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense . . . . [We recognize] that hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners . . . .[2]

> America must also face the rapidly growing threat from cyber-attacks. Now, we know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.[3]

---

[*] Catherine Lotrionte is the Director of the Institute for Law, Science & Global Security and Visiting Assistant Professor of Government at Georgetown University. Dr. Lotrionte has served as Counsel to the President's Foreign Intelligence Advisory Board at the White House and as Assistant General Counsel at the Central Intelligence Agency. Dr. Lotrionte is the Director and Founder of the Cyber Project at Georgetown University and a Life Member of the Council on Foreign Relations.

[1] Secretary-General's High-level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility*, at 11, U.N. Doc. A/59/565 (Dec. 2, 2004) [hereinafter U.N. Report, *A More Secure World*].

[2] DEP'T OF DEF., CYBERSPACE POLICY REPORT 2, 7 (2011) [hereinafter CYBERSPACE POLICY REPORT].

[3] Barack Obama, State of the Union Address (Feb. 12, 2013) (discussing the threats the United States faces from adversaries in cyber and noting the Executive Order that President Obama signed earlier in the day, Executive Order on Improving Critical Infrastructure Cybersecurity, designed to strengthen U.S. cyber defenses through information sharing and standards for cyber security); *see also* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

INTRODUCTION

Few issues in international relations are as controversial as the use of force and the legal framework that justifies a state's use of force in self-defense. Indeed, the very development of the discipline in international law lies in attempts by states, the United Nations, and international courts to wrestle with the question of when force may legitimately be used within the international realm. Over the centuries, states have struggled to define the right to use force as they face new threats from new actors and new weapons entering the arena of conflict.

This Article grapples with the contemporary topic of when a state can invoke forcible measures in cyberspace against non-state actors. To address this issue, this Article discusses the current threats to states that exist in cyberspace, identifies the international law on the use of force and discusses recent state practice as well as the pronouncements of international courts on the topic. Difficult questions in the context of cyber operations are posed and challenging conclusions are drawn from the development of the law. Ultimately, this Article provides a framework for state decision-makers to use to determine whether the state can legally use force in self-defense in cyberspace against non-state actors residing in another state's territory. Overall, it is an indication of the increasing maturity of international law that it is capable of facing up to the complex challenges of these new threats while continuing to search for the path forward that maintains and enhances the rule of law and minimizes conflict within the international community.

It is clear that "cyber warfare" is not a technical legal term and it has been argued by some to be even misleading and unhelpful.[4] There is a concern by some that the term will glorify those criminals responsible for most malicious action in the cyber domain, exaggerate the threat, and distort the understanding of particular conflicts that take place in cyberspace, just as the use of the term "war on terror" arguably has done. Regardless, the rhetoric of "cyber warfare" has some significance for the law on the use of force because it can be used to justify the use of self-defense against other states and non-state actors accused of carrying out a cyber attack against a state.

Today, state officials from around the globe warn that a state's most critical infrastructure—power plants, gas pipelines, traffic control systems, and water

[4] *See, e.g.*, *Cyber Security and International Law: Meeting Summary*, CHATHAM HOUSE 3 (May 29, 2012) (summary of remarks by Mary Ellen O'Connell).

treatment plants—are at risk of attack by adversaries.[5] Military and intelligence officials have repeatedly warned that malicious hackers could disrupt critical infrastructure with the click of a mouse, causing severe economic loss, persistent blackouts or even mass casualties.[6] The issue of how to protect the state from such attacks, internationally, has not been resolved, leaving significant differences between states, and between commentators, on this issue.

In March 2003, the United States argued that Iraq was developing weapons of mass destruction, and undertook *Operation Iraqi Freedom*. The invasion of Iraq was bitterly contested internationally. After the invasion, U.N. Secretary-General Kofi Annan spoke of "a fork in the road" and declared that "this may be a moment no less decisive than 1945 itself, when the U.N. was founded."[7] Questions were raised about the effectiveness of the United Nations, and international law more generally, to deal with new threats. Some states, like the United States, seemed to argue that states were no longer obliged to wait until there was agreement in the Security Council before acting unilaterally or in *ad hoc* coalitions against the terrorist threats.[8] This position represented a fundamental change to the principles on which world peace and stability have been based for the last fifty-eight years under the U.N. Charter framework.

In response, the Secretary-General set up a *High-level Panel on Threats, Challenges and Change*, to examine global peace and security issues, identify how collective security may address these threats, and recommend changes that may be needed. In 2004 the group issued its report, *A More Secure World*.[9] In 2005 the Secretary-General issued his own report, *In Larger Freedom*.[10] In all of these instruments there was a recognition that the nature of twenty-first century threats had changed such that even the most powerful states were vulnerable.[11] However, the consensus from all of the reports was that no change in the U.N. Charter provisions on the use of force was needed. The long-established prohibition on the use of force in Article 2(4) and the right of

---

[5] Obama, *supra* note 3.

[6] *See* text accompanying notes 32–57.

[7] U.N. GAOR, 58th Sess., 7th plen. mtg. at 3, U.N. Doc. A/58/PV.7 (Sept. 23, 2003).

[8] *See, e.g.*, WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 25 (2002).

[9] *Supra* note 1.

[10] U.N. Secretary-General, *In Larger Freedom: Towards Development, Security, and Human Rights for All*, U.N. Doc. A/59/2005 (Mar. 21, 2005) [hereinafter U.N. Secretary-General, *In Larger Freedom*].

[11] U.N. Report, *A More Secure World*, *supra* note 1, at 11.

self-defense in Article 51 were adequate to meet the new threats.[12] Nevertheless, international law on the use of force, its content, application, and effectiveness in dealing with the cyber threats has been the object of much debate.

Indeed, cyber instability poses the same challenge to international peace and security as the threats of terrorism, transnational organized crime, poverty, infectious diseases, environmental degradation, and nuclear, biological chemical, and radiological weapons, as outlined in the U.N. reports.[13] If consensus on the rules related to the use of force in cyberspace is not achieved, the result will be a self-help system within the cyber domain, with potential spillover into the kinetic sphere. Within this domain mistrust will dominate, and opportunities for cooperation for long-term stability and mutual gain will be lost.

The principles related to the use of force have long helped—although not perfectly—world peace and stability. They stand firmly against aggression,[14] facilitate a minimum level of order, and can facilitate a stable basis for exchange, agreement, human creativity, and innovative opportunity in cyberspace. This Article argues that, given the central importance of stability for all states in the cyber domain, the international community must work to preserve the normative principles of *jus ad bellum* and find opportunities to apply these principles in the cyber context. States must work towards a harmonization of what each state understands to be a use of force in cyberspace. Agreement over the contours of sovereignty and self-defense in cyberspace will allow states to develop common terminology, improve predictability, and manage potential crises in the cyber domain.

I. THE CHALLENGES: PRINCIPLES OF SOVEREIGNTY AND SELF-DEFENSE COLLIDE

The challenge in reaching such a new security consensus among states in the cyber domain is multifaceted. First, states may disagree about the nature of the threat in the cyber realm. How one defines the threat will dictate the mechanisms adopted to address the threats. A state may view the cyber threats

---

[12] U.N. Secretary-General, *supra* note 10, at 39; U.N. Report, *A More Secure World*, *supra* note 1, at 55.

[13] U.N. Report, *A More Secure World*, *supra* note 1, at 38–40 (discussing the threats of weapons of mass destruction, terrorism, and transnational organized crime).

[14] Michael N. Schmitt, *Responding to Transnational Terrorism Under the* Jus Ad Bellum*: A Normative Framework*, 56 NAVAL L. REV. 1, 3 (2008).

to be of a criminal nature, carried out by individual hackers, or organized criminal organizations committing fraud and stealing identities online. In this case, the view would be to use criminal law enforcement mechanisms to address the threat. Those that perceive the threat to be a challenge to national power and sovereignty would argue that such a threat requires a response to defend the nation itself.

Second, in cyberspace as in other spaces, states remain sovereign, with rights fully recognized in the U.N. Charter. Even if states recognize the severity and agree on the nature of the cyber threats, they will likely not surrender their fundamental rights. States will still have all the rights of statehood to include the ability to determine whether and to what extent the state will engage with the international community on any security issues. Third, states will maintain the right to exercise self-defense in the cyber domain, as in the domains of air, land, and sea.[15] The cyber domain will not be any different from the other domains in which states have always maintained the right to protect their security. If a use of force is determined to be necessary for their security, states may use force in the cyber context as they would in other domains.

States will remain sovereign in cyberspace. As set forth in the *Island of Palmas* case, the principle of "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[16] By signing the U.N. Charter, states not only benefit from the privileges of sovereignty but also accept certain responsibilities, which include avoiding harm to other states.[17] However, a state's right of sovereignty and its obligation to do no harm, at times, exist in tension. In the cyber context, states exercise sovereign control over cyber infrastructure and cyber operations located within their territory, including the right to limit access to the Internet from within the state.[18] This same principle of sovereignty also includes an obligation by states to respect the sovereignty of other states, including their

---

[15] In 2011, the U.S. government officially stated its position on a State's right of self-defense in the cyber domain, noting that, "[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." *See* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 10 (2011) [hereinafter 2011 INTERNATIONAL CYBERSPACE STRATEGY].

[16] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[17] *E.g.*, U.N. Charter art. 51.

[18] NATO COOP. CYBER DEF. CTR.OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed.) (forthcoming 2013) (manuscript r. 1, para. 10) [hereinafter TALLINN MANUAL], *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft.

territorial integrity.[19] As the International Court of Justice ("ICJ") held in the *Nicaragua* case, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[20] In the cyber context, states have an obligation to prevent their cyber infrastructure from being used by others to harm another state.[21]

Cyber operations against another state's territorial infrastructure can violate a state's sovereignty.[22] Historically, the ICJ has ruled that a state has the right of control over its territory and that other states cannot interfere in the territorial state's freedom to maintain exclusive and independent control over that territory. In the *Corfu Channel* case, the ICJ found that Great Britain had violated the sovereignty of Albania by not obtaining Albania's permission before conducting a mine sweeping exercise in Albanian territorial seas.[23] In addition to violations of a state's sovereignty, depending upon the "scale and effect" of a cyber operation, it could constitute an "intervention," a "use of force," or an "armed attack."[24] All of these designations are international wrongful acts.

States will maintain the right to use force in self-defense in cyberspace. Just as the U.N. Charter recognizes a state's right of sovereignty, the Charter and customary international law fully recognize a state's right of self-defense against threats.[25] The state's right to use force in self-defense, however, is contingent on the nature of the threat.[26] Certainly, if a state has been the victim of an armed attack from another state, the victim state has the right to use force in self-defense against the aggressor state.[27] If a cyber attack is launched from State A and harms State B, the sovereignty of State B has been violated. State A still maintains a right of sovereignty. State B, however, also may have the right of self-defense against State A. In this case, the right of sovereignty of State A is in conflict with State B's right of self-defense.

---

19 *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 202 (June 27).

20 *Id.*

21 TALLINN MANUAL, *supra* note 18 (manuscript r. 5, para. 3).

22 *See id.*

23 Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 36 (Apr. 9).

24 *See Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, para. 195; *see also* U.N. Charter art. 2 (noting a prohibition on use of force and intervention); *id.* art. 51 (noting the right of self-defense in response to armed attack).

25 U.N. Charter arts. 2, 51.

26 *Id.* art. 51.

27 *See id.*

What if, however, a state has been the victim of a cyber attack by a non-state actor operating from within another state's territory? To what extent can the victim state use force within the state where the non-state actor is operating? What is the level of responsibility of the target state for the non-state actor's actions? Unfortunately, both in conventional warfare and in the cyber context, international law has not provided a clear standard for when a victim state may use force in self-defense against a non-state actor. As the U.N. report, *A More Secure World*, urged, "[t]he norms governing the use of force by non-State actors have not kept pace with those pertaining to States. . . . The United Nations must achieve the same degree of normative strength concerning non-State use of force as it has concerning State use of force."[28]

In the cyber domain, where non-state actors can hide with impunity in the territory of a state and launch attacks against other states, states currently lack effective international legal guidance to inform their decisions about using force. This Article explores the roles and responsibilities of states to preserve the fundamental principles of international law that exist to promote stability, security, and peace in the cyber context. By describing how these principles are being challenged today by non-state actors, this Article offers some sense of how the principles of sovereignty and self-defense can co-exist, holding non-state actors accountable, holding states responsible, making victim states safer, and making cyberspace more stable.

There is a significant consensus that international law governs activities in cyberspace and that states maintain sovereignty rights as well as the right to defend against threats in cyberspace.[29] What is less certain is whether, in acting to preserve these rights, states will be well-enough informed to make decisions that not only preserve these rights but also reduce conflict in cyberspace and minimize the opportunity for escalation. Where the international rules in cyberspace are not yet firmly established, decisions related to the circumstances under which a state will use force in cyberspace will be dictated by state practice and customary international law.[30] This customary practice will take time as states consider options and consequences. In the meantime, as such practice begins to develop, this Article recommends a number of

---

[28] U.N. Report, *A More Secure World*, *supra* note 1, at 48.

[29] *See, e.g.*, *infra* notes 134–153 and accompanying text.

[30] *See* Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, International Law in Cyberspace, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) (transcript available at http://www.state.gov/s/l/releases/remarks/197924.htm).

practical, and hopefully, effective criteria for one standard that states could consider when making determinations about when to use force in the context of cyber attacks from non-state actors. In proposing the standard, the ultimate goals of this Article are to increase the security of the cyber domain, minimize the use of force in the domain, provide more predictability of action and uphold the central principles of international law. This Article's intent is to propose a standard that may guide states in honoring the principles of sovereignty, preserving the right of self-defense, and making informed decisions related to national security matters in cyberspace.

II. BENEFITS OF A STANDARD FOR ASSESSING WHEN TO USE FORCE IN RESPONSE TO NON-STATE ACTORS

There are a number of potential benefits to adopting a standard like the one proposed in this Article. The standard offered in this Article is based on fundamental principles of international law and would likely be supported by other states that recognize the same normative principles. Offering a standard that is likely to gain early acceptance at least among like-minded states would help the idea to be recognized quickly by as many states as possible. A standard such as the one this Article proposes can be discussed publicly to gain international agreement on the standard's meaning. This allows for ex post facto assessments of the state's actions in using force. If the U.N. Security Council or an international court were to review a state's actions ex post facto, a state that uses a clear standard to determine whether the use of force was appropriate creates a factual record with unambiguous points of reference that would be uniformly understood by all parties. It may also improve the likelihood that the state's actions will be viewed as legal and legitimate in the eyes of the international community or court.

Particularly for those states that see themselves as victim states with respect to uses of force or armed attacks in cyberspace, a standard against which to evaluate possible responses to cyber attacks would provide the state with a useful decision-making tool, as well as a learning instrument that can be changed as new circumstances may call for repeated use of the standard. This allows a state to learn over time with repeated iterative use of a standard. As there are more instances when states invoke the standard in their decisions to use force in the cyber context, this will provide more opportunities for the standard to be tested. With more use, the standard will likely gather more international acceptance, particularly if the perception is that the stated objectives of the standard were upheld, minimizing conflict and improving

stability and peace in cyberspace. State practice may ultimately coalesce around the standard creating more predictability in cyberspace.

III. THE THREATS FACED IN CYBERSPACE

In June 2010, the then-incoming Secretary of Defense, Leon Panetta, testified before the Senate Armed Services Committee that "the next Pearl Harbor that we confront could very well be a cyberattack."[31] On October 11, 2012, Secretary Panetta gave a speech in New York discussing the Department of Defense's responsibility in cyber-security, describing the threat as a "cyber Pearl Harbor."[32] He provided examples of specific scenarios where a cyber attack could result in physical destruction and loss of life, paralyze and shock the nation, and create a profound new sense of vulnerability.[33] He likened the cyber threats to terrorism, nuclear weapons proliferation, and the turmoil in the Middle East,[34] the same threats the previously mentioned U.N. reports identified as challenging the basic principles of international relations.[35] Most recently, in a speech at Georgetown University, on February 6, 2013, Panetta sounded the alarm about cyber attacks against the United States, describing how foreign cyber actors are probing critical infrastructure and creating "tools to attack these systems and cause panic and destruction and even the loss of life."[36] His speech came on the heels of recent cyber attacks on *The New York Times*,[37] U.S. financial institutions, and the state oil companies of Saudi Arabia and Qatar.[38]

The United States' 2010 *National Security Strategy* cited cyber threats as "one of the most serious national security, public safety, and economic

---

[31] Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack*, CHRISTIAN SCI. MONITOR (June 9, 2011), http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

[32] Sec'y of Def. Leon E. Panetta, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012) (transcript available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136).

[33] *Id.*

[34] *Id.*

[35] U.N. Report, *A More Secure World*, *supra* note 1, at 38–40.

[36] *See Panetta Delivers Sharp Warning About Cyber Attacks*, WASH. FREE BEACON (Feb. 6, 2013 10:26 AM), http://freebeacon.com/panetta-delivers-sharp-warning-about-cyber-attacks/.

[37] *See* Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, N.Y. TIMES, Jan. 31, 2013, at A1.

[38] *See Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow*, REUTERS, Dec. 9, 2012, *available at* http://www.reuters.com/article/2012/12/09/saudi-attack-idUSL5E8N91UE20121209.

challenges we face as a nation."[39] The report described how "[t]he very technologies that empower us to lead and create also empower those who would disrupt and destroy."[40] Certainly, the growth of cyber technology has been a significant driver for economic growth. Unfortunately, it has also been a catalyst for new vulnerabilities for modern society. Cyberspace has empowered people to conduct business across borders in seconds, run power plants through centralized control systems, and even coordinate the movements of troops in distant locations while simultaneously creating new and dangerous opportunities for adversaries to attack these very same operations.[41] As with the technologies of the past, the advances in cyber technology, while originally designed to improve life, are being transformed into instruments for aggression.

As networked computers have proliferated, so too have the threat vectors for potential hacker groups and non-state actors to exploit for economic or political gain.[42] From the theft of individuals' bank account information to a disastrous piece of malware destroying an electrical grid, states and non-state actors have the ability to wreak serious damage on individuals or states alike around the globe with just the click of a mouse.[43] These changes in technology have heralded a new security climate for states—one where opportunities for cooperation exist but are matched with an unprecedented scope for destruction. Within this new environment, there is a growing recognition by a number of states, including the United States, of the need to work through international channels in order to establish security in cyberspace to maintain its benefits for all.[44]

On May 16, 2011, President Barack Obama released the United States' *International Strategy for Cyberspace*.[45] In recognizing the challenges posed by malevolent actors who threaten the security of the Internet, President Obama called upon states to "work towards building the rule of law, to prevent the risks of logging on from outweighing its benefits."[46] In its 2009

---

39 WHITE HOUSE, NATIONAL SECURITY STRATEGY 27 (2010).

40 *Id.*

41 RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 97–101 (2010).

42 WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009) [hereinafter 2009 CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

43 JEFFREY CARR, INSIDE CYBER WARFARE 1–14 (2d ed. 2012).

44 *See* 2009 CYBERSPACE POLICY REVIEW, *supra* note 42, at iv.

45 2011 INTERNATIONAL CYBERSPACE STRATEGY, *supra* note 15.

46 *Id.* at 3.

Cyberspace Policy Review, the Obama administration had concluded that "[i]nternational norms are critical to establishing a secure and thriving digital infrastructure."[47] Most recently, in the State of the Union Address on January 12, 2013, President Obama warned, "[E]nemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems [in cyber]."[48] The President called upon the Congress to work to better secure the networks of the critical infrastructure upon which the United States depends.

In July 2011, the Department of Defense released its *Strategy for Operating in Cyberspace*, noting that cyber attacks could constitute an act of war to which the United States would consider responding with kinetic force.[49] The report stated the U.S. position that the laws related to armed conflict were applicable to cyberspace, and inaugurated the notion of "equivalence" in cyberspace in response to significantly destructive attacks.[50] In other words, if there is harmful action in the cyber domain, it can be met with a parallel response in another domain. In releasing the strategy, former Deputy Secretary of Defense William J. Lynn stated, "[T]he United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing."[51]

The Pentagon's strategy also calls for international engagement concerning what cyber activities will be acceptable to states.[52] In order to minimize the likelihood of inter-state confrontations, an international dialogue and consensus on the appropriate legal responses to threats in cyberspace will become all the more important as states consider kinetic responses to cyber attacks.

On July 26, 2012, General Keith Alexander, the Commander of U.S. Cyber Command, gave the U.S. government's first public remarks about the increase in pace of cyber attacks against the U.S. critical infrastructure.[53] He described

---

47 2009 CYBERSPACE POLICY REVIEW, *supra* note 42, at iv.

48 Obama, *supra* note 3.

49 CYBERSPACE POLICY REPORT, *supra* note 2, at 2

50 *Id.* at 4–5.

51 William J. Lynn, III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy (July 14, 2011) (transcript available at http://www.defense.gov/speeches/speech.aspx?speechid=1593).

52 CYBERSPACE POLICY REPORT, *supra* note 2, at 9.

53 David Sanger & Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. TIMES, July 27, 2012, at A8.

the threat against the U.S. electric grids, water supplies, and banking networks. *The New York Times* cited General Alexander when it reported that "there ha[s] been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations."[54] In the past, General Alexander has also drawn a distinction between what he called *disruptive* cyber attacks, such as denial-of-service attacks aimed at interrupting the flow of communication or finance, and *destructive* attacks designed to destroy parts of the network infrastructure of the United States, like routers and servers.[55] According to General Alexander, a destructive cyber attack against critical infrastructure of the United States could be devastating.[56] These are the types of destructive attacks that have the potential to cause serious long-term damage to the national security of the United States.[57]

The cyber operations against Estonia in 2007, Georgia in 2008, and Iran in 2010 are three of the most recent and most public examples of cyber operations that call for an international cooperative approach—one that combines not only law enforcement, economic, and diplomatic measures but, when appropriate and necessary, military measures.[58] The reality of the cyber domain is that states and non-state actors can and will use cyber weapons to threaten the security of other states. At times, a proportional use of force in response to cyber attacks may be necessary, which would implicate the international laws related to the use of force.

A. The Role of International Law

The rapidly changing structure and undergirding technologies of the global system over the last decade have brought international legal issues to the

---

[54] *Id.*

[55] Cheryl Pellerin, *U.S. Leaders Cite Partnership as Key to Cybersecurity*, AM. FORCES PRESS SERVICE (Oct. 2, 2012), http://www.defense.gov/news/newsarticle.aspx?id=118074 (quoting General Alexander as saying "Over the last few weeks, we've seen distributed denial-of-service attacks, so we're seeing the threat grow from exploitation to . . . disruption, and my concern is it's going to go from exploitation and disruption to destruction" (alteration in original)); *see also* John T. Bennett, *NSA General on Cyberattacks: 'Probability for a Crisis is Mounting,'* U.S. NEWS & WORLD REP. (July 9, 2012), http://www.usnews.com/news/blogs/dotmil/2012/07/09/nsa-general-on-cyberattacks-probability-for-a-crisis-is-mounting.

[56] Pellerin, *supra* note 55; *see also* Bennett, *supra* note 55.

[57] *See* CYBERSPACE POLICY REPORT, *supra* note 2, at 3–4.

[58] *A Look at Estonia's Cyber Attack in 2007*, MSNBC, July 8, 2009, *available at* http://www.msnbc.msn.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack; Parisa Hafezi, *Iran Admits Cyber Attack on Nuclear Plants*, REUTERS, Nov. 29, 2010, *available at* http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129; John Swain, *Georgia: Russian 'Conducting Cyber War,'* TELEGRAPH (Aug. 11, 2008, 11:11 AM), http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

forefront of national policy and international relations in a variety of fields. Cyberspace is no exception. Virtually every international issue from weapons of mass destruction,[59] torture,[60] and cybercrime[61] to environmental protection,[62] airline safety,[63] and trade barriers,[64] is governed by some aspect of international law—whether negotiated agreements, multilateral regimes, or norms of behavior. There is no aspect of international relations that international law does not impact in some way. International law not only protects the status quo, it reflects the aspiration for a stable and productive world order in the face of emerging threats. In the cyber domain, as has long been the case with other domains such as land, air, sea, and space,[65] international law will be a necessary instrument to ensure both international peace and the security and operability of the Internet across national borders.

Cyber conflict is an emerging form of warfare not yet explicitly addressed by international law.[66] Much of the current international law related to conflict was developed at a time when states were the only actors to commit acts of aggression with conventional weapons.[67] Since the end of the Cold War, however, the international community has become acutely aware that the nature of threats in the international community has changed.[68] New weapons

---

[59] *E.g.*, Treaty on the Non-proliferation of Nuclear Weapons, *opened for signature* July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 (entered into force Mar. 5, 1970).

[60] Convention Against Torture and Other Cruel, Inhuman Degrading Treatment or Punishment, Dec. 10, 1984, S. TREATY DOC. NO. 100-20, 1465 U.N.T.S. 85.

[61] *E.g.*, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. No. 185 (entered into force Jan. 7, 2004) (Council of Europe).

[62] *E.g.*, United Nations Framework Convention on Climate Change, *done* May 9, 1992, S. TREATY DOC. No. 102-38, 1771 U.N.T.S. 107 (entered into force Mar. 21, 1994).

[63] Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S 295.

[64] Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154.

[65] *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3, 397; UNITED NATIONS TREATIES AND PRINCIPLES ON OUTER SPACE, U.N. Doc. ST/SPACE/11, U.N. Sales No. E.02.I.20 (1992) (reprinting several U.N. treaties and principles concerning outer space, which set forth the basic parameters for the military use of space, banning weapons of mass destruction, weapons testing, the establishment of military installations in outer space, and forbidding any state from claiming sovereignty over any celestial body).

[66] *See* Kenneth Anderson, *Why a Cybersecurity Treaty is a Pipe Dream, and a Better Approach for New Conflict Technologies*, VOLOKH CONSPIRACY (Oct. 29, 2011, 11:16 AM) http://www.volokh.com/2011/10/29/why-a-cybersecurity-treaty-is-a-pipedream-and-a-better-approach-for-new-conflict-technologies.

[67] DAVID J. BEDERMAN, INTERNATIONAL LAW FRAMEWORKS 52 (3d ed. 2010) ("It used to be that States were the only recognized subjects of international law, the only 'real' players on the international scene."); *see also* Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 119 (2nd Cir. 2010) (describing how, after the Nuremburg Trials, states were no longer the sole focus of international law), *cert. granted*, 132 S.Ct. 472 (2011); *cf.* U.N. Charter art. 3 (opening membership to states, not individuals or organizations).

[68] *See, e.g.*, S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001) (acknowledging changing threats to international peace after September 11, 2001).

such as nuclear weapons and new non-state actors such as terrorists have emerged on the global scene and, at times, have threatened international security.[69] International organizations and courts have responded to these new threats by applying existing international laws and, when necessary, developing new law.[70] The same should be done with cyber threats, whether the cyber threat emerges from states or non-state actors. As the *White House Cyber Strategy* states: "The 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. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[71] This Article follows in this vein as it seeks to further develop the norm of state responsibility with respect to non-state actors in cyber conflict.

Some international legal scholars have argued that cyber security should be regulated by those international laws related to economic and communication issues rather than by those that regulate military conflict.[72] Indeed, most of the contested operations in cyber have been acts of cyber crime, identity and intelligence property theft, and espionage—both economic espionage and classic political espionage.[73] These activities are currently regulated by domestic state laws and, to some extent, international law.[74] There have been

---

[69] *See* Nicholas Watt, *Pakistan Boasted of Nuclear Strike on India Within Eight Seconds*, GUARDIAN (June 15, 2012), http://www.guardian.co.uk/world/2012/jun/15/pakistan-boasted-nuclear-strike-pakistan (illustrating ongoing tension as a result of nuclear weapons). *See generally* Chair of Security Council Committee Established Pursuant to Resolution 1373 (2001), Counter-Terrorism Committee Executive Directorate, Global Survey of the Implementation of Security Council resolution 1373 (2001), transmitted by letter dated Aug. 17, 2011 from the Chair of the Security Council Comm. addressed to the Secretary-General of the General Assembly, U.N. Doc S/2011/463 (Sept. 1, 2011).

[70] *Cf.* U.N. OFFICE ON DRUGS AND CRIME, FREQUENTLY ASKED QUESTIONS ON INTERNATIONAL LAW ASPECTS OF COUNTERING TERRORISM 95–99 (2009), *available at* https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf (describing U.N. guidance to States on reconciling human rights and counter-terrorism measures).

[71] 2011 INTERNATIONAL CYBERSPACE STRATEGY, *supra* note 15, at 9.

[72] *See, e.g.*, CYBER SECURITY AND INTERNATIONAL LAW: MEETING SUMMARY, *supra* note 4, at 3 (remarks of Mary Ellen O'Connell).

[73] MARTIN C. LIBICKI, CRISIS AND ESCALATION IN CYBERSPACE (2012).

[74] The U.S. has criminalized a number of activities related to cyber crime and espionage. *See* Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (2006); Economic Espionage Act of 1996, 18 U.S.C. § 1831 (2006) (listing criminal prohibitions against economic espionage); Convention on Cyber Crime, Nov. 23, 2001, C.E.T.S. No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. The Convention on Cyber Crime was the first international treaty that criminalized specific computer crimes. Forty-seven States are signatories to the Convention. Espionage, universally criminal under domestic laws, does not ipso facto violate international law. *See* ABRAM N. SHULSKY, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE

relatively few instances of cyber conflict compared to the instances of cyber crime and espionage.[75] This Article addresses cyber conflict and not the broader topic of cyber security in the context of telecommunications laws, criminal law, economics or privacy law.[76] This is not to minimize the damage that can be done to a state from cyber crime or espionage. Government and industry experts have illustrated the tremendous losses from organized criminal activities in cyberspace as well as state-run cyber espionage operations against the United States.[77] However, the international laws that control state uses of force, the focus of this Article, do not regulate crime or espionage.

This Article focuses on those cyber threats that challenge the very independence, national power and viability of a state. This Article does not challenge the position that the Internet is and will remain, hopefully, a place for communication, commerce and innovation. This Article recognizes that the Internet will also be a place where states maintain sovereignty and continue to exercise the fundamental right to act in self-defense when threatened. Due to the lack of agreement on the applicability of the rules related to the use of force in cyber, it is imperative to conduct a review of these international principles, to analyze their application in cyber, and to use these principles to build a consensus about appropriate behavior in the cyber domain.

---

103 (2d ed. 1993); Sean P. Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 289 (1996).

[75] Most experts estimate that there have been three to four cases of cyber conflict: the distributed denial-of-service ("DDoS") attacks against Estonia in 2007, the attacks against Georgia in 2008, the Stuxnet worm targeting Iran in 2009 and 2010, and the Israeli cyber attack against the Syrian radar defense system prior to an air strike against a nuclear reactor in 2007. *See* LIBICKI, *supra* note 73, at 16.

[76] *See* TALLINN MANUAL, *supra* note 18. The *Tallinn Manual* looks at how international law norms apply to cyber warfare. Its author's pays particular attention to *jus ad bellum*, the international law governing the resort to force by States as an instrument of their national policy, and *jus in bello*, the international law regulating the conduct of armed conflict). *See generally The Tallinn Manual*, CCDCOE, http://ccdcoe.org/249.html (last visited Feb. 19, 2013).

[77] PONEMON INST., 2012 COST OF CYBER CRIME STUDY 5 (2012) (finding that the average annualized cost of cyber crime for fifty-six organizations was $8.9 million per year, a six percent increase from the study results from the previous year). For a discussion on the negative impact of economic espionage on the United States, see OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011 (2011). *See also* MIKE ROGERS & DUTCH RUPPERSBERG, PERM. SELECT COMM. ON INTELLIGENCE, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (2012) (accusing two of China's largest telecommunications companies, Huawei Technologies and ZTE Inc., of stealing intellectual property from American companies and identifying them as potential vehicles for the Chinese government to spy against the United States).

The international laws related to the use of force are more fully developed in the case of direct acts by a state.[78] However, for non-state actors who carry out armed attacks against states, there is more than a century of state practice that suggests that it is lawful for a victim state to use force against a non-state actor, even if that non-state actor is in another state's territory, as long as the host state is unwilling or unable to stop the threat posed by the non-state actor.[79] By responding to the threat in the territory of another state, the victim state exercises its right of self-defense, holding that state responsible for the harm it suffered. Where the law is less clear, and what this Article hopes to shed light on, is the appropriate standard the victim state should consider when making the determination to use force in another state's territory, targeting non-state actors who have attacked the victim state.

In response to those who would prefer that policymakers and international lawyers reject a military approach to the threats in cyberspace, this Article argues that failing to analyze the relevant international laws related to military conflict in light of the threats would be irresponsible. States will respond in self-defense against those cyber threats that threaten national security, as they have done for centuries against conventional kinetic threats.[80] To recognize this is not to conclude that cyber security is fundamentally concerned solely with military security. Rather, it is to acknowledge the contemporary importance of "cyber warfare." By assessing the normative structure of *jus ad bellum* under the U.N. Charter, analyzing the principles of use of force decisions by international courts, and applying these principles to the cyber context, this Article argues that these norms can serve to minimize military conflict in cyberspace.

By assessing how the laws of international and non-international armed conflict relate to conflict in the cyber domain, this Article attempts to provide some clarity to the debate over a state's legal authority to take action in the cyber domain in self-defense and, thereby, promote peace and security in the cyber realm. Ultimately, this Article searches for common criteria that states should use to decide when the use of force is justified. The very purpose of the international rules described in this Article, which have widespread international support, is to promote international peace and security in the context of conventional warfare whether on land, sea, air, or space. Nothing

---

[78] BEDERMAN, *supra* note 67, at 72.

[79] W. Michael Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 YALE J. INT'L L. 279, 282 (1985); *see also* BEDERMAN, *supra* note 67, at 232.

[80] *See* BEDERMAN, supra note 67, at 232–35.

ought to prevent these same rules from providing the same benefits to states acting in the cyber realm.

Indeed, international organizations, like the U.N. Security Council, can play a central role in managing these conflicts, defining legal uses of force and unlawful acts of aggression in the cyber domain, and identifying when states can be held accountable for the unlawful actions of non-state actors in their territory. International principles contained in treaties such as the U.N. Charter and in customary law can be applied to non-state actors, as well as to states, to maintain international peace and security and minimize the potential for international conflict in cyber. If the ICJ has the opportunity to address issues of uses of force in the cyber domain, it will need to carefully consider the evidence (even though evidence may be difficult to find and assess)[81] of acts of aggression in cyberspace, whether by states or non-state actors, with or without state support. To maintain international peace and security in the cyber domain, the court will need to support a state's right of self-defense against such acts of aggression. If the court fails to do this, not only will the legitimacy of the court be questioned, but it will have failed to act on the opportunity to bring some stability in the cyber domain. If cases of cyber uses of force come before the court, the court's conclusions must be based on both traditional international law and the reality of the threats to international stability that exist today.

Realistically, most progress in establishing principles in this area will not develop from ICJ decisions but from the practice of individual states, at times acting unilaterally, but hopefully working with other states as well. States, as the primary actors in making international law, must actively seek to develop standards that can be applied under international law in the cyber domain. International law develops primarily through international agreements and state practice.[82] Therefore, especially if the United Nations or the international civil or criminal courts do not take the lead in this area, or if their rulings are not effective, it will be up to states to define what those standards will be. The development of normative standards in this area could be through explicit or

---

[81] *See* Deb Shinder, *What Makes Cybercrime Laws So Difficult To Enforce?*, TECH REPUBLIC (Jan. 26, 2011, 12:05 PM), http://www.techrepublic.com/blog/security/what-makes-cybercrime-laws-so-difficult-to-enforce/4997 (describing the difficulty of obtaining evidence of cybercrime); *see also* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 191–207 (2009) (discussing evidentiary issues in cybercrime cases).

[82] *See* Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1800 (2009) (describing the rules of international law as created "primarily through treaties entered into by states or by customary state practice").

implicit agreements between states and, potentially, with Security Council engagement.[83] As states seek international agreement on these norms, this Article proposes an informal standard that states can consider employing when they make decisions about uses of force in the cyber domain.

These or other agreed-upon standards between states would help reduce violent, dangerous conflict in the cyber domain. In practice, they could serve as useful guideposts for victim and target states in a domain where much is not easily visible, uncertainty is guaranteed, and non-state actors are likely to remain important players. In the world today, non-state actors continue actively to threaten states' national security through cyberspace,[84] and those non-state actors and their state supporters know how to take advantage of the limited ability of victim states to prove attribution with one hundred percent certainty.[85] It is therefore critical that states responding to those threats proceed carefully in the face of clear, balanced rules that have the legitimacy of international acceptance.

The transnational nature of cyber operations and their potentially destructive results raise new and important issues regarding state responsibility under international law. Perhaps the most important of these new issues is whether governments must prevent cyber activities by non-state actors within their borders that cause injury to other states. Similar to other transnational activities, computer networks within a state's territory are subject to state control.[86] Two conclusions follow from this. First, if states have control over these activities, one must determine the level of state responsibility for such

---

[83] There are number of on-going diplomatic efforts through the U.N. Governmental Group of Experts, established under the General Assembly, as well as bilateral efforts with the Russians and Chinese in particular. Russia, China, Tajikistan, and Uzbekistan, have jointly proposed a "code of conduct" with regard to "the rights and responsibilities of States in information space." Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14, 2011).

[84] *See Financial Cybercrime a National Security Threat, U.S. Department of Justice Official Warns*, REUTERS, Sept. 21, 2012, *available at* http://blogs.reuters.com/financial-regulatory-forum/2012/09/21/financial-cybercrime-a-national-security-threat-u-s-justice-department-official-warns (equating attacks on U.S. banks with attacks on U.S. national security); *Strategy to Combat Transnational Organized Crime: Protect the Financial System and Strategic Markets Against Transnational Organized Crime*, NAT'L SEC. COUNCIL, http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/financial-system (last visited Oct. 26, 2012) (describing cybercrime as a threat to U.S. security).

[85] *See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINALITY 379, 409–29 (2007) (explaining the difficulty of attributing cyber attacks to a particular attacker).

[86] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 65–86 (2006).

activities when they are destructive to others. When and how should the state be held responsible? What factors will be weighed to determine ultimate state responsibility? These questions must be answered uniformly, especially when states consider using kinetic force in response to malicious cyber actions in their territory. In the absence of these agreed-upon standards, there is a risk of arbitrary response decisions that could have catastrophic consequences, including escalation of conflict in cyberspace. Second, state control implies the need for state cooperation and international engagement among states to achieve effective global cyber security norms.

To achieve stability in the cyber domain, it is paramount that engagement takes place at the government level with the involvement of key non-governmental players. Efforts to harmonize domestic legislation, improve law enforcement collaboration, and socialize norms of state responsibility for cyber security are some of the fundamental first steps to ensuring the Internet remains open, reliable, and secure. Unlike the domains of land, sea, and air that are controlled exclusively by states and international organizations, cyberspace is dependent upon non-governmental organizations, private sector corporations, and individuals for its overall functionality.[87] Several different groups need a seat at the table with states to create international stability and security in the cyberspace: corporations like Google; international nonprofit corporations; organizations like the Internet Society, the Internet Engineering Task Force, and the Internet Corporation for Assigned Names and Numbers ("ICANN"), which develops the Internet's technical protocols and standards; and computer security experts. The absence of these entities from the decision-making process would deprive cyber security development efforts of key players and their needed expertise.[88] This evolution of international private-public cooperation will, therefore, have profound and unique impacts on the practical development of the state responsibility norm in the cyber domain.

Although these international Internet governance bodies will be important partners in ensuring Internet security, their ability to influence the behavior of state actors is limited. These organizations lack any formal lawmaking authority and often have difficult relationships with states, making the development and acceptance of norms promulgated by these organizations

---

[87] *See, e.g.*, Zoë Baird, *Governing the Internet: Engaging Government, Business and Non-Profits*, FOREIGN AFF., Nov.–Dec. 2002, at 18 (describing the key role of ICANN in the functioning of the Internet).

[88] *Cf.* Greg Rattray *The Emerging Global Information Infrastructure and National Security*, 21 FLETCHER F. WORLD AFF. 81, 95 (1997).

challenging.[89] Because states will continue to exercise sovereignty in the cyber domain, it is critical to engage with the state actors to begin to define what acceptable behavior is in that domain. Key states will be the critical actors in establishing principles for cyber conflict and international law is the appropriate framework that will guide state behavior in cyberspace.

Today international laws do not specifically address the rules related to state action and a state's responsibility in cyberspace. These laws will ultimately be shaped by state practice. By drawing upon already well-established international norms related to conflict however, and further developing norms such as state responsibility, states can develop lasting rules for conduct in cyberspace that contribute to improved world order.

B. The Cyber Domain Under International Law: How Sovereignty Remains Relevant

Some analysts have compared the Internet to either a global public good or a global commons.[90] While both comparisons have relevant implications for cyber activities under international law, and therefore are useful comparisons in the cyber context, both terms ought to be recognized as imperfect applications in the cyber domain. Public goods are commodities that are non-rival and non-excludable—that is to say, there is zero cost associated with extending the service to an additional person, and it is impossible or expensive to exclude individuals from enjoying it.[91] Because these goods benefit everyone, only the government can typically provide these goods and benefits to the public. Any private company that may have had an interest in providing such goods to the public quickly recognizes its inability to charge for the goods and therefore loses any interest in providing the goods.

While the cyber domain and access to the Internet are similar to public goods in that they are readily available to everyone at little-to-no cost, the

---

[89] Eric Engleman, *Commerce Department Keeps ICANN as Web's Address Manager*, BLOOMBERG (July 3, 2012), http://www.bloomberg.com/news/2012-07-02/u-s-commerce-department-retains-icann-as-web-s-address-manager.html (describing tense negotiations between the U.S. government and ICANN).

[90] JOSEPH S. NYE, JR., THE FUTURE OF POWER 143 (2011) (describing the Internet as a public good); *see also* Joseph S. Nye, Jr., *The American National Interest and Global Public Goods*, 78 INT'L AFF. 233, 241 (2002); Gregory J. Rattray, Chris Evans, & Jason Healey, *American Security in the Cyber Commons*, *in* CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 137–76 (Abraham M. Denmark & James Mulvenon eds., 2010) (discussing whether cyberspace can be considered a global commons).

[91] Rattray, Evans & Healey, *supra* note 90, at 14–15.

physical infrastructure of the Internet can be costly to develop and maintain securely.[92] Importantly, this infrastructure can be physically located within sovereign states that have the ability to disconnect from the Internet (e.g., China's Great Firewall), preventing access for many.[93] The principle of sovereignty implies that a state has the right to control access to its territory, and therefore, can limit any Internet access within its sovereign territory. Such a capability undermines the Internet's designation as a commons—something that cannot be owned by one person. Unlike the high seas, which are a "pure" commons for all humanity and are not controlled by any one state,[94] the cyber domain is an "imperfect commons"[95] over which states have sovereign authority to exclude others and enforce domestic rules that have an impact on the Internet beyond its borders.

As an "imperfect public good," ensuring the availability and security of the Internet is a complex problem to deal with under international agreements, where global exclusion is difficult and exploitation by one party can subtract value for other parties and threaten the national security of states.[96] Providing security for this complex system will ultimately require state involvement, but the danger is that governmental protection may lead to fragmentation of the Internet where states decide to wall themselves off from the Internet in an attempt to insulate their societies from the dangers that travel through the Internet.[97] China, for instance, has developed the ability to disconnect from the Internet if attacked and still operate internally on its own domestic form of the Internet.[98] The United States may also be developing plans to maintain the ability to disconnect from the Internet.[99]

---

92 Ross Anderson, *Why Internet Security Is Hard—An Economic Perspective*, ANN. COMPUTER SEC. APPLICATIONS CONF. (2001) (describing Internet security in the context of the global commons).

93 Katia Moskovich, *Cracks in the Wall: Will China's Great Wall Crack*, BBC NEWS (May 1, 2012), http://www.bbc.co.uk/news/technology-17910953.

94 HUGO GROTIUS, THE FREEDOM OF THE SEAS (James Brown Scott ed., Ralph van Deman Magoffin trans., Oxford Univ. Press 1916) (1663).

95 NYE, *supra* note 90, at 143.

96 *Id.* (stating that cyberspace is an "'imperfect commons' or a condominium of joint ownership without well-developed rules.").

97 A number of States have developed the capability to disconnect from the Internet. Examples of States that have been able to at least partially shut down Internet access are: Buram during the attempted revolution in 2008; China in 2009 after the riots in the province of Xinjiang; Iran in 2009 during the post-election Green Movement protests; and Syria in June 2011 during protests against the government. REBECCA MACKINNON, CONSENT OF THE NETWORKED 51–52 (2012).

98 CLARKE & KNAKE, *supra* note 41, at 146.

99 Declan McCullagh, *Renewed Push To Give Obama an Internet "Kill Switch,"* CBS NEWS (Jan. 24, 2011), http://www.cbsnews.com/8301-501465_162-20029302-501465.html (noting that the proposed legislation that would have contained the "kill switch" authority was not passed by Congress).

States like China and the United States, however, have a lot to lose by disconnecting from the Internet. If China were to cut itself off from the Internet, this would negatively affect China's export ability. China would likely face a withdrawal of Western investors as the Internet cutoff would result in a significant financial loss for Western investors.[100] States, in recognizing the economic benefits of the international connectivity of the Internet, would be wise to develop disconnect plans only as a last resort in the face of a profound threat.

The Chinese government also controls domestic access to content on the Internet by maintaining control over the mechanisms by which information travels through the Internet, through the Great Firewall of China. By filtering Internet traffic through eight gateways that connect the Chinese Internet to the global Internet and configuring Internet routers at those gateways to block certain website addresses and keywords, the Chinese government can prevent information from entering China that it deems threatening to its own regime.[101]

As with pure public goods and true commons under international law, the principle of sovereignty is a significant political hurdle to securing the Internet for all across national boundaries. Similar to a public good, there is no effective market for government action that can solve the problem of Internet security; there is no process for global citizens to make collective decisions to secure the Internet.[102] Contrary to what some, like John Perry Barlow, may have envisioned or wished for, during the early years of the Internet, cyberspace was not a place where no rules existed. Barlow and others discussed the Internet as a place where there was no sovereignty, a space that existed outside of government control where individual users on the Internet would form a "social contract" to solve problems and provide for any needs.[103]

Under a system of sovereign states, the states have the power and legal authority to establish laws and institutions within their territories to provide for national public goods—such as Internet access—as well as to take action to ensure the safety and welfare of the nation and its citizens.[104] If a state determines that harmful effects are impacting individuals or entities within the state because of information that flows from the Internet into that state, that

---

100 LIBICKI, *supra* note 73, at 100.

101 MACKINNON, *supra* note 97, at 35.

102 *See* GOLDSMITH & WU, *supra* note 86.

103 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FREEDOM FOUND. (Feb. 8, 1996), http://homes.eff.org/~barlow/Declaration-Final.html.

104 GOLDSMITH & WU, *supra* note 86, at 156.

state could take action to prevent that flow of harmful information, including cutting off access to the Internet. "A government's responsibility for redressing local harms caused by a foreign source does not change because the harms are caused by an Internet communication."[105]

China and Russia[106] see internal dissent and anti-government writings disseminated on the Internet as one of the greatest online threats, and they maintain their authority to censor such information and limit access to the Internet.[107] The United States, on the other hand, has argued against "overbroad state control" of the Internet, stating that Internet should not be "a system dominated by centralized government control."[108] Because of Chinese and Russian state sovereignty, however, the United States cannot force them to grant Internet users the right to voice their opinions. Contrary to what some argued about the nature of the Internet, the Internet exists in the real world where states continue to maintain sovereign control.

The 2009–2010 controversy between the Chinese government and Google illustrates two significant facts about the current role of states and the "new digital superpowers" of the Internet—companies such as Google, Facebook, Microsoft, and Twitter. First, it illustrates how states will assert their sovereign right to control what takes place within their territory to include the cyber domain, and how states must balance that exercise of control with the goal of maintaining economic prosperity by continuing to reap the benefits of being connected to the Internet. Importantly, it also illustrates how the development of the norm of state responsibility will depend on cooperation between the government and private sector.

In January 2010, Google announced that it would stop complying with censorship of searches by Google.cn and no longer do business within

---

105 *Id.*

106 China and Russia are not the only States that regulate content on the Internet in the name of protecting national security. *See* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5 (Ronald Deibert et al. eds., 2008) The report found that twenty-six of the forty countries tested, including South Korea, China, Saudi Arabia, Tunisia, Iran and Yemen, filtered citizens' Internet access in 2005 and 2006. *Id*.

107 *E.g.*, *Russia Passes Bill Modeling China's 'Great Firewall,'* GBTIMES (July 12, 2012), http://gbtimes.com/news/russia-passes-bill-modeling-chinas-great-firewall.

108 Michael H. Posner, Assistant Sec'y for the Bureau of Democracy, Human Rights, and Labor, Remarks on Internet Freedom and Responsibility (Oct. 25, 2011), *available at* http://www.state.gov/j/drl/rls/rm/2011/176144.htm; *see also* Francis Tan, *US in New Push To Break China's Internet Censorship*, NEXT WEB (May 11, 2011), http://thenextweb.com/asia/2011/05/11/us-in-new-push-to-break-chinas-internet-censorship.

China.[109] This declaration came in response to attacks from Chinese computer servers, accessing the Gmail accounts of some human-rights activists, infiltrating some thirty-three companies' networks, and likely stealing Google source code.[110] Throughout the controversy, the Chinese government denied knowledge of the attacks while also maintaining its claim to the right to control the cyber domain within its sovereign territory, citing the supremacy of Chinese law within its cyber territory.[111]

After the incident, Google announced that it would no longer cooperate with the Chinese government in its efforts to censor search results and would remove its censorship of certain items from its Chinese network.[112] Prior to the cyber attacks, Google had been following China's law with respect to required censorship.[113] When Google announced it would stop abiding by the China censorship agreement, the Chinese government accused Google of evading Chinese law.[114] From the perspective of the Chinese government, if Google refused to abide by the censorship orders from the Chinese government based on the domestic laws of the state, Google would not do business in China.[115] Ultimately, Google retained its license to do business in China and continued some activities not related to search (e.g., Android mobile phone operating system development and support, advertising sales, and research and development).[116] Pressure within China from businesspeople who argued that a total ban on Google would be detrimental to Chinese industries that rely on Google's products and services was instrumental to the Chinese government's decision not to order a complete ban on all Google services.[117] Google and the Chinese government came to a mutual agreement as to the terms of how Google would continue to do business within China.[118]

---

[109] Tania Branigan, *Google To End Censorship in China over Cyber Attacks*, GUARDIAN (Jan. 12, 2010), http://www.guardian.co.uk/technology/2010/jan/12/google-china-ends-censorship.

[110] Timothy L. Thomas, *Google Confronts China's "Three Warfares,"* PARAMETERS, Summer 2010, at 101, 101.

[111] For a discussion of China's claim to sovereignty in cyberspace, see Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1585–87 (2010).

[112] SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 117–18 (2011); *see also* Thomas, *supra* note 110, at 104.

[113] Thomas, *supra* note 110, at 106.

[114] *Id.* at 104.

[115] MACKINNON, *supra* note 97, at 7–8.

[116] *Id.* at 8.

[117] *Id.* at 8–9.

[118] David Barboza & Miguel Helft, *A Compromise Allows Both China and Google To Claim a Victory*, N.Y. TIMES, July 10, 2010, at B1.

Google was not the only corporation that faced disagreements with the Chinese government but ultimately submitted to China's domestic laws. In 1999, as Yahoo! entered the Chinese market, it announced that Yahoo! China would "give Internet users in China easy access to a range of Yahoo!'s popular services . . . ."[119] However, the Chinese government demanded that Yahoo! filter materials the government deemed potentially harmful or threatening to the regime's rule.[120] In the summer of 2002, Yahoo! agreed to China's demands and signed the *Public Pledge on Self-Discipline for the Chinese Internet Industry* and agreed to "inspect and monitor the information on [Chinese] domestic and foreign Web sites" and "refuse access to those Web sites that disseminate harmful information in order to protect the Internet users of China from the adverse influence of the harmful information."[121]

In defense of the company's actions, and in response to critics who dubbed Yahoo! a "Chinese police auxiliary,"[122] Jerry Yang, Yahoo! founder and former CEO, noted that, "[t]o be doing business in China, or anywhere else in the world, we have to comply with local law."[123] Similarly, Google acknowledged the challenge of doing business globally: "[Google] cannot run a business in China without being physically in China."[124] Companies that do business in other states will be subject to the sovereign authority of that state and its domestic laws. Cyberspace is no different than other domains where the sovereignty of the state persists. Companies, like Yahoo! and Google, face a difficult choice: abide by the states laws or forgo doing business within that state. Companies, just like states, must balance the advantages and disadvantages of these choices.

While the Yahoo! and Google cases are largely commercial disputes between corporations and the state in which they conduct business, they also have clear political and international implications. Highlighting the political significance of the Google incident, U.S. Secretary of State Hillary Clinton, in a speech on January 21, 2010, spoke out about the Google incident, articulating

---

119 Press Release, Yahoo!, Yahoo! Introduces Yahoo! China (Sept. 24, 1999), *available at* http://docs.yahoo.com/docs/pr/release389.html.

120 Sumner Lemon, *Yahoo Criticized for Curtailing Freedom Online*, PCWORLD (Aug. 12, 2002, 7:00 AM), http://www.pcworld.com/article/103865/yahoo_criticized_for_curtailing_freedom_online.html.

121 *Id.* (alteration in original) (internal quotation marks omitted).

122 *"Living Dangerously on the Net,"* REPORTERS WITHOUT BORDERS (May 12, 2003), http://en.rsf.org/article.php3?id_article=6793.

123 Peter S. Goodman, *Yahoo Says It Gave China Internet Data; Journalist Jailed By Tracing E-mail*, WASH. POST, Sept. 11, 2005, at A30.

124 GOLDSMITH & WU, *supra* note 86, at viii.

the U.S. commitment to freedom of communications in digital networks and calling on China to "conduct a thorough review of the cyber intrusions . . . ."[125] This embarrassed China and increased tensions between the two nations.[126] Chinese news outlets said Secretary Clinton's singling out of China was inappropriate and misguided and constituted an inappropriate meddling in Chinese affairs.[127] For Google, the implications were financial rather than political, and the dispute was resolved accordingly, with business decisions in mind.[128] From the U.S. government's perspective, however, there were larger political issues at stake that called for the establishment of new norms for the Internet to be adopted by states: norms of state responsibility in the cyber context.[129] For Secretary Clinton, it was important to point out that China could be held responsible for attacks within its territory against U.S. companies. From the financial reputations of corporations to the economic and political security of states, a great deal is at stake in the cyber domain.

As with other public goods in the international community, under international law, states cannot coerce other states to accept the costs of providing public goods without their consent. In the absence of any treaty agreement, the only international legal mechanism capable of coercing free-riding states to accept solutions to ensure Internet access would be state unanimity at the U.N. Security Council. Within the U.N. system, members of the United Nations "confer on the Security Council primary responsibility for the maintenance of international peace and security."[130] This authority of the Security Council extends into the cyber realm.[131] If the Security Council were to determine that there has been a "breach of the peace," an "act of aggression," or a "threat to the peace," it could authorize measures to restore international order.[132] This would extend into cyberspace. Such actions

---

[125] Hillary Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010) (available at http://www.state.gov/secretary/rm/2010/01/135519.htm).

[126] VAIDHYANATHAN, *supra* note 112, at 118.

[127] *See* Paul McDougall, *China Defends Great Firewall*, INFORMATIONWEEK (Jan. 22, 2010), http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222400246.

[128] VAIDHYANATHAN, *supra* note 112, at 117–21 (arguing that Google merely "chose the more profitable of the two evils") (citing *Does Google Violate Its 'Don't Be Evil' Motto?*, NPR (Nov. 26, 2008), http://www.npr.org/templates/story/story.php?storyId=97216369).

[129] Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, ATLANTIC COUNCIL 5 (Jan. 2012), http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibility Cyber.PDF.

[130] U.N. Charter art. 24.

[131] Nils Melzer, *Cyberwarfare and International Law*, UNIDIR 6 (2011), http://unidir.org/pdf/activites/pdf2-act649.pdf.

[132] U.N. Charter art. 39.

authorized or mandated by the U.N. Security Council under Chapter VII of the U.N. Charter would not constitute a violation of the target state's sovereignty since the United Nations was acting under its granted authorities.[133] Although the U.N. Security Council has the authority to mandate Internet security and Internet access if it deems it necessary to the maintenance of international peace and security, such a determination is not likely to occur. Unanimity among the permanent members of the Security Council, in light of the divergent views on Internet access and content control among states, is quite unlikely.

Indeed, contemporary international law gives each state a right to be free, independent, and uninhibited from foreign control and forcible coercion. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648,[134] holds that each state retains exclusive authority over activities within its borders.[135] The principle of state sovereignty over national territory is a basic tenet of international law, universally accepted as customary international law.[136] This customary rule of territorial sovereignty is codified in modern international law.[137] Any limitation on the authority a state has over its territory is subject to the consent of the state. Without the state's consent, no other state may use force within the territorial state. Whether by land, sea, or air, no state may invade or use armed force within the sovereign territory of

---

133 TALLINN MANUAL, *supra* note 18, (manuscript r. 1, para. 7) ("Security Council-mandated or authorized actions under Chapter VII of the United Nations Charter (Rule 18), including those involving cyber operations, do not constitute a violation of the target State's sovereignty.").

134 *See* BEDERMAN, *supra* note 67, at 2.

135 *See infra* notes 136–39.

136 Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 842 (2001) (citing Statute of the International Court of Justice art. 30(1)(b), June 26, 1945, 59 Stat. 1031; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 202 (June 27); Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), at 121, U.N. Doc. A/RES/2625 (XXV) (Oct. 24, 1970) [hereinafter Declaration on Friendly Relations]; Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131 (XX), at 12, U.N. Doc. A/RES/2131 (XX) (Dec. 21, 1965) [hereinafter Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States]; RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 (1987)).

137 The principle of territorial sovereignty was first codified in 1919 in Article 10 of the Covenant of the League of Nations. League of Nations Covenant art. 10 ("The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League."). The Charter of the United Nations reaffirms the principle of territorial integrity in Article 2(4). U.N. Charter art. 2, para 4 ("All Members [of the United Nations] 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.").

another state.[138] The scope of this authority over territory covers all national space, including cyberspace.[139]

Although information contained in the cyber realm may be located in a "cloud" and the full stream of information flow may not travel through national territory per se, the physical aspects of cyberspace, such as computers, servers, phones, and fiber optic cables, are owned by a state or by private companies that operate in accordance with a state's laws, and such assets are located within the borders of a governed state territory.[140] The fact that a state's physical cyber assets located in its territory are connected to the global Internet does not waive a state's territorial sovereignty over those cyber assets and the activities involving them.[141] The principle of sovereignty extends to the state's authority over these assets, providing the state the right to restrict or protect access to the Internet.[142] States maintain sovereignty over cyber assets within the state's territory, and therefore these cyber assets are subject to the state's legal and regulatory control and are protected by the state's territorial sovereignty.[143] As the state exercises such authority over its cyber assets, it also has certain obligations that follow from its sovereign authorities under international law.

The principles of sovereignty and territorial integrity as rights of a state do not exist in a vacuum, but are balanced against the right of self-defense under international law.[144] As the principle of sovereign equality conveys certain rights and exclusive authorities on a state, it also entails the obligation of all states to respect the territorial sovereignty of other states and prevent harm to them.[145] In accordance with the U.N. General Assembly's *Declaration*

---

138 Joyner & Lotrionte, *supra* note 136, at 843.

139 *See* Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 17 (2009) ("[C]yberspace is part of the 'real' world and thus subject to its constraints and order—in other words, subject to state sovereignty."); *see also* Kanuck, *supra* note 111, at 1573–74.

140 Gabriel M. Scheinmann & Raphael S. Cohan, *The Myth of "Securing the Commons,"* WASH. Q., Winter 2012, at 115, 124.

141 TALLINN MANUAL, *supra* note 18 (manuscript r. 1, para. 10).

142 *Id*. at 25–27.

143 *Id.* at 25.

144 *See* BEDERMAN, *supra* note 67, at 272.

145 *See* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (separate opinion of Judge Alvarez) ("Sovereignty confers rights upon States and imposes obligations on them."); *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 202 (June 27) (quoting *Corfu Channel*, 1949 I.C.J. at 35) ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations."); TALLINN MANUAL, *supra* note 18 (manuscript r. 5, para. 2); *cf.* Stephen Allen, *Harboring or Protecting? Militarized Refugees, State Responsibility, and the Evolution of Self-Defense*, 25 PRAXIS: FLETCHER J. HUM. SECURITY 5, 9–10 (2010).

Concerning Friendly Relations, states have a duty to refrain from organizing, encouraging, assisting, or tolerating incursions of armed bands or acts of civil strife in another state, and a duty to refrain from armed intervention for any reason in the internal or external affairs of another state.[146] Under international law, states have an obligation to take appropriate steps to protect the interests of other states, including criminal acts or other activities that inflict serious damage to the victim state.[147]

The idea is that when one state violates another state's territorial integrity, it forfeits its own right to territorial integrity and state sovereignty. For example, if State A knows of a plan to conduct cyber attacks from its territory that will cause damage within State B's territory and does not take reasonable steps to prevent this from occurring, then State A forfeits its rights of sovereignty within its territory as State B's right of self-defense is activated. Within the legal context of rights, there exists a "balance between one State's right to territorial integrity and another's right to self-defense . . . ."[148] How these rights are balanced between two states will depend on how a state invoking the right of territorial integrity has complied with international obligations with respect to the other state. The governance of the Internet and securing nations from cyber attacks, like providing for public goods and the protection of the commons under international law, bring this balance between sovereignty and a state's duties under the law to the forefront of the debate.

International law also requires that states "use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people . . . ."[149] It is well established, for example, that a state will be responsible for damage emanating from its territory, whether caused by noxious fumes, attacks by terrorists or mines exploding in waterways.[150] These obligations stem from the basic principle of sovereignty, which entails both rights and obligations for states. Every state has the right to dictate what takes place within its territory; however, that right ends where another state's

---

146 *See* Declaration on Friendly Relations, *supra* note 136, at 121.

147 United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, paras. 68–69 (May 24); *see also* Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905 (1941).

148 Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 540 (2003).

149 S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7) (Moore, J., dissenting) (citing United States v. Arjona, 120 U.S. 479 (1887)).

150 *Trail Smelter*, 3 R.I.A.A. at 1965–67. For a related responsibility of states, see *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 4, 22–23 (Apr. 9) (noting that Albania was obligated to notify British authorities of "the existence of a minefield in Albanian territorial waters and [to warn] the approaching British warships of the imminent dangers to which the minefield exposed them").

territory begins. The right of sovereignty under international law declares intolerable any active intrusion into the internal affairs of a state. Article 2(4) of the U.N. Charter, by prohibiting one state from using or threatening to use force against another state, is a written and codified source of this obligation.[151]

In the cyber domain, a host-state that has both the capability to prevent a cyber attack emanating from its territory, causing harm in another state, and fails to take action to prevent that harm has failed to fulfill its duty under Article 2(4) of the U.N. Charter. A cyber operation that constitutes a use of force under Article 2(4) is an internationally wrongful act.[152] This proposition is reinforced when the host-state openly supports the cyber attack after the fact and fails to punish those individuals responsible. As the U.S. *International Cyber Strategy* states, in the cyber domain as in the physical domain, states need to recognize and act on their legal responsibility "to protect information infrastructures and secure national systems from damage or misuse."[153]

The events of 9/11 were perhaps the most pivotal point in history with regard to the evolution of the norm of state responsibility under international law. The international community, including the international legal community, was faced with the concrete reality that the world faced new threats, from non-state actors specifically, and that there was a need to rethink international legal mechanisms for dealing with these threats. The attacks against the United States on September 11, 2001, illustrate the ability of non-state actors to carry out attacks against a state, causing significant death and destruction. Non-state actors in the cyber domain have also illustrated their ability to cause great harm to states.[154] The vast majority of cyber attacks that have occurred to date have not been carried out by state-sponsored hackers, but by criminals intending to steal intellectual property and financial information.[155] The level of connection between such criminals and a state is debatable. And although the cyber attacks that have occurred to date likely would not constitute an armed attack under the U.N. Charter framework,

---

151 U.N. Charter art. 2, para. 4.

152 *See id.*

153 2011 INTERNATIONAL CYBERSPACE STRATEGY, *supra* note 15, at 10.

154 *See generally* Gregory J. Rattray & Jason Healey, *Non-State Actors and Cyber Conflict*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 69–74 (Kristen M. Lord & Travis Sharp eds., 2011) (describing the history of non-State actors in cyber attacks).

155 2009 CYBERSPACE POLICY REVIEW, *supra* note 42, at 2.

unlike the 9/11 terrorist attacks, future cyber operations could cause the level of destruction necessary to constitute an armed attack.

In the aftermath of the 9/11 attacks, there was a major departure from prior state practice in countering threats by non-state actors. Through a unanimous resolution, the U.N. Security Council authorized states to respond to the attacks carried out by al Qaeda with lethal force within the territory of another sovereign state.[156] Whether a non-state actor could conduct an "armed attack" under international law has long been debated by international law scholars.[157] The U.N. Security Council, by invoking Article 51 of the U.N. Charter against those who carried out the 9/11 attacks, implied that attacks by non-state actors, in fact, could trigger the right of self-defense under the U.N. Charter.[158]

Traditionally under international law, legal duties are imposed on a sovereign state only with its consent.[159] Furthermore, the actions of private non-state actors are not attributable to the state.[160] Liability for non-state actions would attach to the state only if the non-state actor is either a formal or de facto agent of the state.[161] The ICJ has held in the context of military operations, that a state is responsible for the acts of non-state actors when it has "effective control" over such actors.[162] However, there is disagreement over how much "control" is necessary to find a non-state actor's actions attributable to a state. In *Prosecutor v. Tadić*, the International Criminal Tribunal for the Former Yugoslavia ("ICTY") adopted an "overall control" test,[163] which is

---

156 *See* S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 11, 2001); *see also* U.N. Report, *A More Secure World*, *supra* note 1, at 18.

157 *See infra* notes 209–212.

158 Special Rapporteur on Extrajudicial Summary or Arbitrary Executions, *Report of the Special Rapporteur on Extrajudicial Summary or Arbitrary Executions: Addendum*, Human Rights Council, paras. 40–41, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston) [hereinafter *Report on Extrajudicial Executions*].

159 LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 27 (1995) ("State consent is the foundation of international law. The principle that law is binding on a state only by its consent remains an axiom of the political system, an implication of state autonomy.").

160 *See* Rep. of the Int'l Law Comm'n, 53d Sess., April 23–June 1, July 2–Aug. 10, 2001, at 80, U.N. Doc A/56/10, U.N. GAOR, 56th Sess., Supp. No. 10 (2001) ("Thus the general rule is that the only conduct attributed to the State at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e. as agents of the State.").

161 *Id.*

162 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 15 (June 27).

163 Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, para. 120 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

considered a less stringent threshold.[164] However, even with this lower standard, the ICTY found that the control would have to go "beyond "the mere financing and equipping of such forces and involv[e] also participation in the planning and supervision of military operations."[165] And yet, after 9/11, international law held Afghanistan accountable because it failed to uphold its duties to prevent al Qaeda from harming other states from its territory.[166] Furthermore, Afghanistan was held liable for terrorists attacks carried out by a non-state actor that no one argued was an agent of Afghanistan.

Under international law, these responses to the 9/11 attacks considerably altered the application of *jus ad bellum* and, importantly, the norm of state responsibility. In the wake of those terrorist attacks, the United States argued that the attacks constituted an "armed attack" within the meaning of the self-defense provision of Article 51 of the U.N. Charter.[167] As mentioned above, the issue of whether acts of non-state actors can constitute an armed attack absent direction by a state was controversial. Traditionally, Article 51 of the U.N. Charter and customary law of self-defense were characterized as applicable solely to armed attacks undertaken by one state against another.[168] Violent acts by non-state actors fell within a criminal law framework.[169]

The United States further argued that it had the legal authority to act in self-defense against Afghanistan because the Taliban, the ruling regime of Afghanistan, had supported and harbored leaders of the perpetrators of the 9/11 attacks—al Qaeda.[170] In other words, the Taliban had failed to take action to prevent al Qaeda from launching attacks against the United States from Afghanistan, despite U.S. pressure to do so.[171] Through explicit warnings

---

164 *See generally* Antonio Cassese, *The* Nicaragua *and* Tadić *Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 EUR. J. INT'L L. 649 (2007) (comparing the "overall control" test to the "effective control" test and explaining why the less stringent overall control test is appropriate in certain circumstances where the more stringent effective control may not be appropriate).

165 *Id.* para. 145.

166 *See* S.C. Res. 1378,U.N. Doc. S/RES/1378 (2001) (Nov. 14, 2001).

167 Ashley S. Deeks, *Pakistan's Sovereignty and the Killing of Osama Bin Laden*, AM. SOC'Y INT'L L.: INSIGHTS (May 5, 2011), http://www.asil.org/pdfs/insights/insight110505.pdf.

168 *Report on Extrajudicial Executions*, *supra* note 158, paras. 40, 46.

169 *Id.* para. 46 ("Traditionally, States have refused to acknowledge the existence of an armed conflict with non-state groups. The reasons include not wanting to accord such groups recognition as 'belligerents' or 'warriors', and instead being able to insist that they remain common criminals subject to domestic law.").

170 Permanent Rep. of the U.S. to the U.N., Letter dated Oct. 7, 2011 from the Permanent Representative of the United States to the United Nations addressed to President of the Security Council, U.N. Doc. S/2001/946 (Oct. 7, 2001).

171 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 350 (2004) ("The United States had warned the Taliban that they would be held accountable for further attacks by Bin

provided by the Unites States, the Taliban knew about the threat of harm that al Qaeda posed from within its territory, yet failed to meet its obligations under international law to prevent harm to others. Because there was no indication that the Taliban had directed al Qaeda in its operations against the United States, according to the reasoning of prior international court decisions, the Taliban did not "exercise[] effective—or even overall—control over al Qaeda."[172] Nevertheless, the United States concluded that because the Taliban had provided sanctuary to al Qaeda (refusing to expel its leader, bin Laden) even after being warned, the United States concluded that al Qaeda's actions on 9/11 were imputable to the Taliban government.[173]

In essence, the right of sovereignty that Afghanistan possessed under international law was balanced against the United States' right of self-defense. Under the circumstances where Afghanistan failed to meet it international obligations, which resulted in harm to the United States, the United States' right to use force in self-defense prevailed under international law. Following the 9/11 attacks, state responsibility for the actions of non-state actors can follow from the state's failure to meet its international obligations to prevent its territory from being used as a platform or sanctuary for the non-state actors to attack other states.[174]

Counterterrorism policy after 9/11 heralded in an important shift in the norm of state responsibility under international law. In authorizing the use of force against the al Qaeda in Afghanistan, the U.N. held Afghanistan responsible, in part, for al Qaeda's attack against the United States. States are now held responsible for failing to prevent terrorists within their territory from causing harm elsewhere. As with counterterrorism policy, state practice in cybersecurity may reflect a similar adoption of the notion of a state's obligations vis-à-vis non-state actors under international law.

IV. INTERNATIONAL LAW ON THE USE OF FORCE

This Part of the Article provides an overview of contemporary U.N. Charter law and customary international law governing the use of force by

Ladin against Afghanistan's U.S. interests. The warning had been given in 1998, again in late 1999, once more in the fall of 2000, and again in the summer of 2001.").

172 David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 96 (2010).

173 *See* Vincent-Joël Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing To Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L. L. 615, 637–41 (2005).

174 *See* TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 3 (2006).

states in self-defense. In 1945, the United Nations was created "to save succeeding generations from the scourge of war" and "to suppress acts of aggression or other breaches of the peace."[175] Any analysis of the international laws related to the use of force begins with the prohibition on the use of force in Article 2(4) of the UN Charter.[176] States and commentators frequently use the word "war," as is apparent in the language often used in discussing "cyber war," but the drafters of the U.N. Charter purposely chose to use the broader term "use of force" in the prohibition in Article 2(4). States generally agree this prohibition is not only a treaty obligation but also customary international law.[177]

Under international law there are a number of well-established exceptions to this general prohibition against the use of force: consent by a sovereign state;[178] authority of the U.N. Security Council under Chapter VII, Articles 39, 42 and 48;[179] self-defense under Article 51 of the U.N. Charter;[180] and anticipatory self-defense in accordance with the necessity and proportionality requirements of the *Caroline* precedent.[181] In addition, most scholars recognize that there are uses of force that would fall below the threshold of Article 2(4), and therefore would not constitute a violation of Article 2(4).[182] While such actions below the Article 2(4) threshold would not constitute uses of force, they may, however, constitute violations of other principles of international law such as sovereignty and the norm of non-intervention.

The language of the U.N. Charter, as drafted in 1945, imposes certain challenges on the application of its provisions to contemporary cyber conflicts. First, there is the difficulty in determining the specific meaning of the words as used in the Charter given that the Charter does not define a "use of force" for

---

175 U.N. Charter pmbl.; *see also* Oscar Schachter, *International Law: The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1620 (1984) ("When the United Nations . . . Charter was adopted, it was generally considered to have outlawed war."). For more information on the founding of the United Nations, see Joyner & Lotrionte, *supra* note 136, at 845.

176 U.N. Charter, art. 2 para. 4.

177 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 190 (June 27).

178 U.N. Report, *A More Secure World*, *supra* note 1, at 58.

179 U.N. Charter arts. 39, 42, 48.

180 *Id.* art. 51.

181 *See* R.Y. Jennings, *The* Caroline *and* McLeod *Cases*, 32 AM. J. INT'L L. 82, 89 (1938) (noting that the right of anticipatory self-defense is recognized in customary international law).

182 *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 80–81 (Cambridge Univ. Press, 5th ed. 2011).

purposes of Article 2(4)[183] or "armed attack" for purposes of Article 51.[184] Although one may imagine that the intent of the drafters of the Charter meant for the terms "use of force" and "armed attack" to reflect equivalent actions, international tribunals have treated these terms as different concepts.[185] Furthermore, the Charter lacks any express correlation between the terms used in Article 2(4) ("use of force"), Article 51 ("armed attack"), and Article 39 ("act of aggression") of the U.N. Charter, and the seemingly related term, "intervention," noted in a number of General Assembly resolutions.[186] The lack of clear definitions results in disagreement over the application of the law. For instance, the issue of whether "armed attack" is legally synonymous with "aggression" has never been settled.[187]

Second, the U.N. Charter does not address the role of non-state actors in conflict. The Charter was developed as a response to the Second World War and was therefore focused on inter-state conflict, not the role of non-state actors in conflict.[188] The issue of the scope of the applicability of Articles 2(4) and 51 to non-state actors was not addressed by the Charter. Nor does the Charter resolve the questions of a victim state's right of self-defense against a non-state actor. In addition, at the time of the drafting of the Charter, there was no way for nations to consider the types of weapons that would be used in today's conflicts. Cyber weapons like nuclear weapons were not even considerations in the minds of the drafters of the Charter. Today, states must

---

183 *See* U.N. Charter, art. 2, para. 4.

184 *Id.* art. 51. Article 51 reads:

> Nothing 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, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Id.

185 *See* JAMES A GREEN, THE INTERNATIONAL COURT OF JUSTICE AND SELF-DEFENCE IN INTERNATIONAL LAW 111–28 (2009); TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 53–68 (2010).

186 *E.g.*, Definition of Aggression, G.A. Res. 3314 (XXIX), Annex, arts. 1–3, U.N. Doc. A/RES/3314 (XXIX) (Dec. 14, 1974); *see also* G.A. Res. 42/22, Annex, para. 1(7), U.N. Doc. A/RES/42/22 (Nov. 18, 1987); Declaration on Friendly Relations, *supra* note 136, Annex, at 123.

187 As defined by the U.N. General Assembly, "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition." Definition of Aggression, *supra* note 186, Annex, art. 1.

188 CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 7 (3d ed. 2008).

address the use of advanced cyber weapons in the context of conflicts, determining the legality of their use. Weapons such as trojan horses, viruses, worms and logic bombs have the potential to cause instantaneous and overwhelming damage to the functioning of a state while preserving the anonymity of the adversary. In contemporary times, where conflict will be conducted through cyberspace with cyber weapons, debates on law and policy related to issues of the role of non-state actors, attribution, responsibility, sovereignty, intervention, use of force and self-defense will dominate discussions.

Imagine that a state is the targeted victim of a cyber attack from a private organization, a terrorist organization, or a privately owned security company, located within another state. Under this scenario, does the victim state have any recourse against the state from which the attack originated or against the private organization? Has the private organization committed an international wrongful act for which it can be held responsible? Can the state from which the private entity acts be held accountable for the private entity's actions? Has the private entity violated Article 2(4) of the U.N. Charter for which it can be held responsible? Some scholars have argued that Article 2(4) of the U.N. Charter applies solely to members of the United Nations and "do[es] not apply to the acts of non-state actors, including individuals, organized groups, and terrorist organizations, unless they were attributable to a state pursuant to the law of state responsibility."[189] These scholars argue that if the act can be attributable to the state then the state is held to be in violation of the prohibition on the use of force and not the non-state actor.[190] This interpretation of the U.N. Charter places the state as the sole entity of analysis.

For purposes of Article 51 of the U.N. Charter and the customary law of self-defense, traditional international law characterized these principles as only applicable to states that had undertaken armed attacks against another state.[191] Under this view, it is argued that the drafters of the Charter meant to cover only states when referring to Article 51.[192] The terrorist attacks of 9/11 and the specific response to those attacks, however, have raised questions about the legal doctrine of self-defense as it applies to non-state actors. The issue of

---

189 TALLINN MANUAL, *supra* note 18 (manuscript r. 10, para. 5).

190 *Id.*

191 *Id.* (manuscript r. 13, para. 16).

192 Antonio Cassese, *The International Community's 'Legal' Response to Terrorism*, 38 INT'L & COMP. L. Q. 589, 597 (1989); Eric P.J. Myjer & Nigel D. White, *The Twin Towers Attack: An Unlimited Right to Self-Defence?*, 7 J. CONFLICT & SECURITY L. 5, 7 (2002).

whether Article 51 extends to attacks by non-state actors in the absence of any state complicity has been controversial in modern international law.

Recently, scholars have disputed the position that only states can commit the kinds of actions that constitute an "armed attack" as envisioned in Article 51 of the U.N. Charter. These scholars have argued that the U.N. Charter provisions were intended to cover non-state actors as well.[193] Others who support this position argue that there has been an expansion of the law after 9/11, permitting forcible self-defense against states harboring terrorists.[194] There has been much debate among academics about what it means for terrorist action to be attributable to a state.[195]

Prior to 9/11, only a few states had invoked the principle of self-defense to justify the use of force in response to non-state terrorist attacks.[196] In response to 9/11, however, state practice indicated a shift in states' positions on this issue and a willingness by a number of states to apply the right of self-defense to attacks conducted by non-state actors.[197] Following the 9/11 attacks, the Security Council, for the first time, implicitly affirmed the right of self-defense in response to terrorist attacks in Security Council Resolution 1368.[198] Some have expressed doubt as to whether the resolutions passed by the Security

---

193 Rein Müllerson, Jus ad Bellum*: Plus ça Change (Le Monde) Plus C'est L Même Chose (Le Droit)?*, 7 J. CONFLICT & SECURITY L. 149, 182 (2002).

194 Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J.168, paras. 4–15 (separate opinion of Judge Simma) (arguing that the armed attacks carried out by irregular forces from States that do not have effective control over their territory still constitute armed attacks. They argued that 9/11 had brought about changes in the law); *id.* at 29–30 (separate opinion of Judge Kooijmans) (same); *see also* Steven R. Ratner, Ius ad Bellum *and* Ius in Bello *After September 11*, 96 AM. J. INT'L L. 905, 906 (2002).

195 *E.g.*, STANIMIR A. ALEXANDROV, SELF-DEFENSE AGAINST THE USE OF FORCE IN INTERNATIONAL LAW 182 (1996); ANTHONY CLARKE AREND & ROBERT J. BECK, INTERNATIONAL LAW AND THE USE OF FORCE: BEYOND THE UN CHARTER PARADIGM 158 (1993) (describing four levels of State sponsorship of terrorist actors: none, toleration, support, sponsorship).

196 *See* ALEXANDROV, *supra* note 195, at 182; AREND & BECK, *supra* note 195, at 142, 158. Prior to 9/11, Israel and the United States had invoked Article 51 to justify the use of force in response to terrorist attacks abroad: by Israel against Tunis in 1985, AREND & BECK, *supra* note 195, at 152; by the United States against Libya in 1986, ALEXANDROV, *supra* note 195, at 184; by the United States against Iraq in 1993 in response to an attempted assassination against former President Bush by Iraqi agents; *Id.* at 186; and by the United States against Afghanistan and Sudan in 1998, RUYS, *supra* note 185, at 202.

197 After the 9/11 attacks by al Qaeda, the U.N. Security Council adopted a number of resolutions recognizing the applicability of the right of self-defense. *See* S.C. Res. 1368, *supra* note 156; S.C. Res. 1373, *supra* note 68. One could argue that by "recognizing the inherent right of individual or collective self-defence in accordance with the Charter" when condemning the terrorist attacks on 9/11 in Resolution 1368 and invoking the specific language of Article 51 in doing so, the U.N. Security Council affirmed the right of self-defense against non-State actors when there has been an "armed attack." *See* S.C. Res. 1368, *supra* note 156.

198 S.C. Res. 1368, *supra* note 156.

Council after 9/11 actually support a legal right of self-defense against terrorists because the language expressly used in the resolutions is "threat to international peace and security" rather than "armed attack" under Article 51.[199] Furthermore, they argue that because the language invoking the right of "self-defense" was mentioned only in the preamble of the resolutions and not in the legally controlling resolution articles, the Council was not affirming the existence of any such right.[200]

It would seem that these arguments are too rigid. First, Security Council resolutions have significance in the development of the law if they deal with state behavior and implicitly or explicitly accept or reject state claims of self-defense. Although Article 51 indicates a central role for the Security Council, it does not require it to rule on the legality of any claim of self-defense, and in practice, it has rarely made explicit reference to Article 51 in its resolutions.[201] When the Security Council has invoked Article 51, it has typically done so in only general terms.[202] Moreover, related to the U.S. claim of self-defense after 9/11, it would seem the Security Council and the international community was willing to accept the use of force in self-defense against the terrorists. Soon after the Security Council resolutions, NATO invoked Article 5,[203] the OAS invoked collective self-defense,[204] Russia, China, and Japan provided military

---

199 Antonio Cassese, *Terrorism is also Disrupting Some Crucial Legal Categories of International Law*, 12 EUR. J. INT'L L. 993 (2001).

200 *Id.*

201 *See* S.C. Res. 546, para. 5, U.N. Doc. S/RES/546 (Jan. 6, 1984) (Security Council affirming Angola's right to take measures in accordance with Article 51 when it was attacked by South Africa); S.C. Res. 574, para. 4, U.N. Doc. S/RES/574 (Oct. 7, 1985) (same); S.C. Res. 661, pmbl., U.N. Doc. S/RES/661 (Aug. 6, 1990) (affirming Kuwait's right to individual and collective self-defense after the Iraqi invasion).

202 S.C. Res. 1234, pmbl., U.N. Doc. S/RES/1234 (Apr. 9, 1999) (recalling the inherent right of individual and collective self-defense in accordance with Article 51 as it related to the conflict in the Democratic Republic of the Congo).

203 Press Release, NATO, Statement by the North Atlantic Council, NATO Press Release (2001) 124 (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm. Article 5 of the North American Treaty provides:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

204 Terrorist Threat to the Americas, C.M.F.A. Res. 24/01, OAS Consultation of Ministers of Foreign Affairs, 24th Meeting, OAS Doc. OEA/Ser.F/II.24/RC.24/RES.1/01 (Sept. 21, 2001).

support,[205] and the United States and United Kingdom wrote to the U.N. Security Council under Article 51, stating that they were acting in individual and collective self-defense.[206] And lastly, to argue the lack of a right to self-defense based upon the decision-making processes of the Security Council ignores strong arguments for a customary right of self-defense, pre-dating the U.N. Charter[207] and underestimates the importance of vast state practice on the issue. The core essence of a right of self-defense is universally accepted.[208]

The question remains as to whether the events following 9/11 brought about a radical transformation of the law of self-defense against non-state actors or whether their significance ought to be narrowly understood. The latter idea is premised on the belief that the actions against al Qaeda after 9/11 were in reaction to a specific incident of terrorist attacks within the territory of a state, leading to a particular response based on Security Council authorization and broad international acceptance by other states. It is currently debated whether any incident in the cyber domain would (no matter how devastating) elicit a response equivalent to the U.S. response to the 9/11 attacks. As with other areas of international law, state practice will likely dictate how the law will develop in this area.

In arguing that non-state actors are indeed covered by Article 51 of the U.N. Charter, one perspective, embraced by the ICJ, is that non-state actors may commit "armed attacks" for purposes of Article 51, triggering the right of self-defense, but only in cases when those attacks are attributable to a state.[209] For instance, when the state is complicit in the non-state actor's actions. Another approach also in support of the view that non-state actors are covered

---

205 Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 96 AM. J. INT'L L. 237, 248 (2002).

206 *See* Permanent Rep. of the U.S. to the U.N., *supra* note 170; Chargé d'affaires a.i. of the Permanent Mission of the U.K. to the U.N., Letter dated Oct. 7, 2001 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2001/947 (Oct. 7, 2001).

207 *See generally* D.W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW (1958); MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER (1961); STEPHEN M. SCHWEBEL, *Aggression, Intervention and Self-Defense in Modern International Law*, *reprinted in* JUSTICE IN INTERNATIONAL LAW: SELECTED WRITINGS 530 (1994).

208 Oscar Schacter, *Self-Defense and the Rule of Law*, 83 AM. J. INT'L L. 259, 259 (1989).

209 *See, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, para. 139 (July 9) (rejecting Israel's argument based on self-defense because Israel had not claimed that the terrorist attacks were imputable to a state); Allen S. Weiner, *The Use of Force and Contemporary Security Threats: Old Medicine for New Ills?*, 59 STAN. L. REV. 415, 435–36 (2006) (mentioning that the international community has been critical of uses of force against non-State terrorists in the territory of another State when the State is not supporting them).

by Article 51, and one taken up by this Article, accepts that an attack by a non-state actor may constitute an "armed attack" regardless of whether a state is directly involved in any aspect of the attack.[210] In support of this position, is the plain language of Article 51, which does not limit the right of self-defense as applicable only to states. Unlike Article 2(4), which specifically refers to a use of force by one "Member" against "any state," Article 51 makes no mention of any requirement of an armed attack being committed by a state.[211] This perspective is also supported by recent state practice in response to terrorist attacks.[212]

In applying this perspective to contemporary cyber operations, this Article argues that devastating cyber operations conducted by a non-state actor against a state which result in the requisite level of harm, equivalent to the scale and effects of an armed attack in the kinetic context, can constitute an armed attack against the state for purposes of Article 51.[213] Moreover, the state would have the right of self-defense against the non-state actor within the territory of the other state. The thornier question, however, is what standard decision-makers should use in deliberating about what factual circumstances would allow for such actions under the law. The Part V of this Article will offer such a standard.

The approach one supports with respect to Article 51 of the U.N. Charter, the right of self-defense, and its applicability to non-state actors will ultimately dictate what one accepts as a legal use of force in response to an "attack" by a

---

[210] *See* JUTTA BRUNNÉE & STEPHEN J. TOOPE, LEGITIMACY AND LEGALITY IN INTERNATIONAL LAW 296 (2010) ("[I]nternational practice seems to have evolved both to allow self-defence against armed attacks by non-state forces, and to loosen the required link between such forces and a state in which armed defence measures are taken."); DINSTEIN, *supra* note 182, at 224–30; Thomas M. Franck, *Terrorism and the Right of Self-Defense*, 95 AM. J. INT'L. L. 839, 840 (2001); Raphaël Van Steenberghe, *Self-Defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?*, 23 LEIDEN J. INT'L L. 183, 184 (2010) (concluding that recent State practice suggests that attacks committed by non-State actors constitute armed attack sunder Article 51).

[211] Sean D. Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 HARV. INT'L L.J. 41, 50 (2002).

[212] *See id.* at 49–50; *see also* Franck, *supra* note 210, at 840 ("It is inconceivable that actions the Security Council deems itself competent to take against a nonstate actor under Articles 41 and 42 in accordance with Article 39 should be impermissible when taken against the same actor under Article 51 in exercise of a state's 'inherent' right of self-defense.").

[213] TALLINN MANUAL, *supra* note 18 (manuscript r. 13, para. 16). *But see id.* ("A minority of the Group [of Experts] did not accept this premise."). The Group of Experts was split over whether individuals, not party to an organization, could conduct armed attacks. Some argued that if the effects of the actions met the scale and effect test then actions of individuals could rise to the level of armed attacks. Others maintained that cyber attacks conducted by individuals were solely matters of criminal law enforcement. *Id.* (manuscript r. 13, para. 19).

non-state actor. Each view will lead to a different test assessing the legality of the use of force. Although the ICJ does not support the third view as described above,[214] this Article argues that this approach is the most appropriate in the context of cyber operations, based on interpretation of the law, past state practice against terrorists and the likely accepted practice by states in cyber conflict. In cyberspace, where disruptive effects against critical infrastructure can be destructive to a state and non-state actors have the capability to carry out damaging cyber operations against states within seconds, if not milliseconds, states will want to react to attacks quickly and effectively.[215]

The remainder of this Article will review the body of international law related to the use of force, examining the relevant factors that treaty law, international courts, and legal scholars have looked to in discussing the legality of the use of force in self-defense. The Part IV of this Article will provide a list of factors as part of a standard that could be used as policymakers contemplate the use of force against a non-state actor conducting cyber attacks from another state's territory in the cyber realm. When a state is addressing the issue of groups conducting cyber attacks against it from within another state, a standard by which to assess the legal bounds for a response in self-defense would be useful.

A. The International Court of Justice: Use of Force Decisions

In 1945, the U.N. Charter established the ICJ as the "principal judicial organ of the United Nations."[216] The Court was to resolve disputes brought before it by states, including disputes related to armed conflict.[217] The U.N. Security Council, through its authorities embodied in the U.N. Charter, also was meant to play a role in resolving disputes as it carried out its function of "maintaining international peace and security." For instance, the U.N. Security Council may, under Chapter VII of the Charter, authorize a state or group of states to use force when it finds that there is a threat or breach of the peace.[218] Since the creation of the United Nations, the Security Council has only rarely authorized such use of force. Under circumstances when the Security Council

---

214 *See supra* note 209 and accompanying text.

215 *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 229–31 (2002) (noting that states should be able to defend against computer network attacks—up to the limits of proportionality—whether or not classified as uses of force, and reviewing both active and passive defense options).

216 U.N. Charter art. 92.

217 *See* BEDERMAN, *supra* note 67, at 233–34.

218 U.N. Charter arts. 39, 41.

fails to take such action, the issue of whether a use of force was lawful is brought before the ICJ. It is important to understand the court's analysis in these cases in order to apply its reasoning to other incidents that will likely occur in the cyber domain.

Since the Court's first rulings related to the use of force, the court has addressed fundamental questions about the application of the following principles:

> To what extent may a state use force in response to acts of violence by another state that fall short of full-scale military campaigns?
>
> To what extent may a state use force in response to non-state actors?
>
> Under what circumstances is a state responsible under international law for supporting or tolerating the presence of non-state groups that use force against another state?
>
> To what extent can force be used against a state that provides such support or tolerance to non-state actors?
>
> To what extent must a resort to force in self-defense be limited in terms of its intensity or scope?

The decisions by the court in these cases address important issues about the resort to force in the absence of Security Council authorization. While these decisions are not without criticism, they provide a reference for the analysis of the international rules that will be the most conducive to the peaceful resolution of conflicts in the cyber domain. These decisions are also useful is assessing the ability of international law and international courts to maintain order in the cyber domain while giving due regard to the legitimate needs of states to protect their basic security interests.

The first dispute to be brought before the court, the *Corfu Channel* case, involved a dispute over the duty of a state to not allow it's territory to be used to harm another state.[219] The case arose out of an incident in October 1946 in which two British destroyers struck mines while passing through Albanian waters in a strait used for passage between areas of the high seas.[220] Albania denied any responsibility for the laying of the mines.[221] After considering the

---

[219] BEDERMAN, *supra* note 67, at 43.
[220] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 12–15 (Apr. 1949).
[221] *Id*. at 11.

facts presented by the parties, the court concluded that the mine laying could not have occurred without the knowledge of the Albanian government.[222] In other words, the Albanian government must have known that the mines had been laid in the channel and was therefore, the court concluded, responsible for its failure to warn the British navy of the presence of the mines and the potential damage to ships.[223] Having known of the threat and failing to alert the British ships to the potential danger from the mines, Albania was found legally responsible for any damages.[224]

The court's opinion is limited in that it did not find that Albania committed an act of aggression. Nor did the court discuss the use of force specifically. It is significant, however, that the court upheld the principle of holding states responsible for acts within its territory that it ought to have known about and that ultimately harmed another state.[225] The court stated that all states have a duty "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[226] From the court's ruling, states can be held responsible for acts of omission that lead to harm irrespective of whether the state's actions rise to the level of a use of force.

The court's decision has been generally well-received.[227] Importantly, it has furthered the development of the law with respect to state responsibility and has been viewed by many as appropriate in holding Albania responsible for its illegal use of force in mining the international strait.[228] However, the part of the court's ruling against Great Britain, finding that Great Britain had violated the sovereignty of Albania by passing through the territorial waters of Albania, in violation of innocent passage, as it swept for mines without

---

222 *Id*. at 22.

223 *Id*.

224 *Id*. at 23.

225 *See id* at 22–23.

226 *Id.* at 22.

227 *See, e.g.*, Quincy Wright, Editorial Comment, *The Corfu Channel Case*, 43 AM. J. INT'L L. 491, 515–16 (1949) ("The Court manifested the tendency, displayed by Chief Justice Marshall in dealing with the American Constitution and by the Permanent Court of International Justice in dealing with the League of Nations Covenant, to construe the rights and powers of the Organization with which the Court was connected broadly enough to permit that Organization to function and to achieve its purposes. International lawyers who recognize that . . . will welcome this tendency of the Court. In a world, shrinking but inadequately regulated, . . . it is probably safer to treat the claims of the international society liberally, even if such treatment . . . involves some danger of stimulating revolt by the states least aware of the situation.").

228 John Norton Moore, Jus Ad Bellum *Before the International Court of Justice*, 52 VA. J. INT'L L. 903, 918 (2012).

Albania's consent, has been criticized.[229] The court, holding Albania responsible for damages, found that Great Britain was also responsible for violating international law.[230] Importantly, this aspect of the court's decision also provides insight into how the court may assess a state's right of self-defense against non-state actors.

By finding that Great Britain violated Albanian sovereignty,[231] some writers argued, the court undermined the law against illegal mining by removing the defensive right of Great Britain.[232] In the cyber context, the implication from the court's ruling is that if a state illegally is conducting cyber operations from its territory in violation of the victim state's sovereignty, the options for other states are to accept the status quo and suffer the consequence of the cyber operations or to respond by using "active defense"[233] measures within the territory of the target state and be condemned equally with the aggressive cyber state.

In 1984, the ICJ was asked for the first time in *Military and Paramilitary Activities in and Against Nicaragua* to resolve a dispute related to a major armed conflict that was currently ongoing.[234] Nicaragua initiated the action in the court alleging that the United States had violated the U.N. Charter, other treaties, and customary international law related to non-intervention and the use of force by carrying out covert operations against Nicaragua, including the mining of Nicaragua waters and training, arming, supplying, and financing the contra rebels who were fighting against the Nicaraguan government.[235] In June 1986, the court ruled in Nicaragua's favor and held that the United States had violated international law.[236] For the first time, the court outlined a distinction between a "use of force" and an "armed attack" as identified in Article 2(4) and 51 respectively in the U.N. Charter.[237]

---

229 *Id.* at 905, 918 (arguing that the ICJ's jus ad bellum decisions have "adopted a minimalist approach undermining the Charter and encouraging aggression, particularly aggression in the 'secret warfare' spectrum").

230 *Corfu Channel*, 1949 I.C.J. at 36.

231 *Id.* at 34.

232 *See, e.g.*, Moore, supra note 228, at 918.

233 *See infra* note 362 and accompanying text.

234 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 32 (June 27).

235 *Id.* para 15.

236 *Id.* para 290.

237 *Id.* para 210.

In the *Nicaragua* decision, the court limited a state's right of self-defense by finding against the United States. The Court rejected the United States' argument that it had acted in collective self-defense on behalf of El Salvador in response to Nicaragua's attacks.[238] The United States argued that the Nicaraguan regime's support of the rebels fighting against the government in El Salvador amounted to an "armed attack" against El Salvador.[239] The court, however, found that Nicaragua's actions in support of the rebels did not rise to the level of an "armed attack" under Article 51 of the U.N. Charter and, therefore, the United States had no right of collective self-defense.[240]

The court used the definition of aggression provided in the *General Assembly's Definition of Aggression* to arrive at its conclusion that "the sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another state of such gravity as to amount to (*inter alia*) an actual armed attack conducted by regular forces, or its substantial involvement therein" could be an "armed attack."[241] In analyzing the actions of Nicaragua and the United States, the court drew a distinction between "the most grave forms of the use of force (those constituting an armed attack)" and "other less grave forms."[242] The latter were still unlawful and could result in declaratory relief or reparations, but only the former entitled the victim to take forcible action in self-defense.

Later on in the *Oil Platforms* case, the court would again invoke the distinction it drew in the *Nicaragua* case between a use of force and an armed attack.[243] The United States has criticized the court's position on this point. Critics have argued that:

> [The] requirement that an attack reach a certain level of gravity before triggering a right of self-defense would make the use of force more rather than less likely, because it would encourage states to

---

238 *Id.* para. 238.

239 *Id.* para. 48, 128.

240 *Id.* para. 230, 235. The Court also found that the collective self-defense principle requires the victim State to provide notice of the attack and publicly ask for assistance in self-defense. The Court failed to find evidence of El Salvador providing such notice or public request for help and ruled against the U.S. claim under collective self-defense. *Id.* para. 199, 236.

241 *Id.* para. 195 (quoting Definition of Aggression, G.A. Res. 3314 (XXIX), art. 3(g), Annex, U.N. Doc. A/RES/3314 (Dec. 14, 1974)) (internal quotation marks omitted).

242 *Id.* para 191.

243 Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 324, para. 51 (Nov. 6).

> engage in a series of small-scale military attacks, in the hope that they could do so without being subjected to defensive responses.[244]

The reverse concern is that, if we conflate the two levels the *Nicaragua* court set up, an armed attack will be as serious as a use of force. The danger in this scenario is that, with no gravity requirement for an armed attack and self-defense, an inter-state conflict could arise out of minor cross-border incidents or other minor uses of force. In a September 2012 speech, Harold Koh, the then-Legal Advisor at the State Department, stated that in cyber space the United States' view is that, "there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[245] He noted that some nations do not agree with this position and consider an "armed attack" as having a higher threshold before the right of self-defense is triggered.[246] In cyberspace, where escalation may occur more quickly with less opportunity for deliberation and deterrence to work, the issue of what thresholds states believe exist related to the use of force, armed attack, and self-defense becomes a very critical issue.[247]

In *Nicaragua*, the court concluded that the actions of Nicaragua and United States did not rise to the level of an armed attack and therefore did not trigger either state's right to use force in self-defense. The court's limited definition of "armed attack" has drawn much criticism, mainly by U.S. writers.[248] Judge Schwebel from the United States and Judge Jennings from the United Kingdom, in their dissenting opinions of the court decision, strongly criticized the court's narrow definition of "armed attack." Judge Schwebel was concerned that the court's decision would encourage predator states to take advantage of weaker states, aggressively acting against them while the victim state would be restricted from legally acting in defense.[249] Other critics of the court's opinion have argued that defining armed attack so narrowly precludes a lawful defensive action in the context of a "secret war" because "assistance to rebels in the form of the provision of weapons or logistical or other support"

---

[244] William H. Taft, IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 295 (2004).

[245] Koh, *supra* note 30.

[246] *Id.*

[247] *See generally* LIBICKI, *supra* note 73.

[248] *See, e.g.*, Thomas M. Franck, *Some Observations on the ICJ's Procedural and Substantive Innovations*, 81 AM. J. INT'L L. 116, 120 (1987); Moore, *supra* note 228, at 953–57; *see also* John Norton Moore, *The* Nicaragua *case and the Deterioration of World Order*, 81 AM. J. INT'L L. 151, 154 (1987).

[249] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 177 (June 27) (Schwebel, J., dissenting).

are components of most secret wars.[250] In the cyber context, this aspect of the court's holding is likely to remove the right of defense against secret warfare, "indirect aggression," and "war by proxy" in cyberspace. This potentially creates an unstable environment in cyberspace where states are encouraged to use cyber methods covertly in a domain where most actions are already conducted in secret. This situation could likely undermine the Charter structure itself.

According to the court, sending armed bands into the territory of another state by itself does not amount to an "armed attack" unless the scale and effects of doing so would be equivalent to "an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces."[251] In applying the reasoning of the court to the 2010 Stuxnet worm that targeted uranium enrichment infrastructure in Iran,[252] the cyber operation would not rise to the level of an armed attack because the malware did not cause any permanent physical destruction equivalent to that level of destruction that "regular armed forces" would have caused nor did it result in any loss of life. In the Stuxnet case, about one thousand centrifuges had to be replaced but there was not any permanent physical damage to the overall facility and there was no loss of life.[253] Temporarily stopping the functioning of the uranium enrichment facility by causing the malfunction of some centrifuges without any serious damage to the facility or loss of life would not be an "armed attack" under the standard outlined by the court in the *Nicaragua* case.[254] Furthermore, under the *Nicaragua* ruling, Iran would not have any forcible right of self-defense under Article 51 of the U.N. Charter.

In some important ways, the decision of the court illustrates a very limited understanding of the requirements of effective war against covert attack and secret wars. This could be particularly troubling in cyberspace where

---

[250] Moore, *supra* note 228, at 928 (quoting *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, para. 195).

[251] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, para. 195.

[252] *See* Jonathon Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets,'* BBC News (Sept. 23, 2010), http://www.bbc.co.uk/news/technology-11388018.

[253] *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

[254] Judge Simma's suggestion in the Oil Platforms case that while "full-scale" self-defense is limited to the "considerably high" threshold of Article 51, a State may take "strictly defensive military action" against lower-level attacks. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 324, paras. 12–13 (Nov. 6) (separate opinion of Simma, J.). In the case of Stuxnet, according to Judge Simma's reasoning, as long as the defensive response was strictly defensive, Iran may legally respond to Stuxnet even if Stuxnet is not considered an armed attack.

attribution of the adversary may be difficult and proxies more easily used by states. In finding that the U.S. action was not necessary in defending El Salvador, the court implies that the United States and El Salvador could have defended El Salvador without violating the sovereign territory of Nicaragua by limiting action to the elimination of the traffic of arms and ammunition inside El Salvador's territory.[255] Particularly in cyber, where it is easy for adversaries to carry out devastating attacks in secret through the use of proxies, a judicial ruling that geographically limits the victim state's right of defense to its own territory will make it extremely difficult, if not impossible, for a state to defeat cyber aggressors. Restricting a state that is under a cyber attack to focus only on incoming traffic once it has crossed the "gateways" at the state's borders provides the aggressor the advantage while leaving the victim state a sitting duck. If a state waits until the adversary has infiltrated its networks with cyber weapons before taking action, it is too late.

B. Support or Tolerance of Non-State Actors

1. State Responsibility Generally

Under customary international law of state responsibility, states bear responsibility for any act that is attributable to the state that is a breach of an international legal obligation applicable to that state.[256] As the *Corfu Channel* case held, such breaches can be both affirmative acts by the state and acts of omission.[257] In the cyber context, an internationally wrongful act that a state would be responsible for could be a violation of the U.N. Charter, a state's use of force through a cyber operations, a violation of a law of armed conflict obligation such as a cyber attack against civilians or the breach of peacetime rules such as conducting cyber operations in the territory of another state without that state's consent. The victim state must be able to show that damage has occurred (or will occur) from the wrongful act.[258] This obligation by the state is not limited to preventing acts that would be criminally harmful to another state, but also extends to acts that would (or have the potential to) inflict serious damage within the victim state.[259]

---

255 *See Military and Paramilitary Activities in and Against Nicaragua*, 1985 I.C.J. 14, para. 154.

256 Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, art. 1–2, U.N. Doc. A/RES/56/83, Annex (Dec. 12, 2001).

257 Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 23 (Apr. 9).

258 *Id.* at 18.

259 Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1980 (1941).

In addition to being internationally wrongful, the act must be attributable to a state. This attribution requirement of the norm is the element that is most challenging in the cyber context. Attribution for cyber operations is particularly difficult when attackers can hide their identity as well as the point of origin of the attack, using neutral states from which to launch the attacks. According to the customary international law of state responsibility, any actions by a state official would be attributable to the state if the individual in question were acting in his or her official capacity.[260] This would include actions that may not have been officially authorized as well as actions conducted by private parties retained by the state.[261] These entities are treated as extensions of the state.

What happens, however, when non-state actors who operate separately from the state conduct a wrongful act in breach of international law? Can such actions be attributable to the state such that the state would incur international legal responsibility for those actions? Under some circumstances, the conduct of non-state actors may be attributable to a state and will give rise to that state's international legal responsibility. According to Article 8 of the Articles of State Responsibility, restating customary international law, such actions can be attributable to a state for legal responsibility purposes if the state has instructed the non-state actors to take specific action or provided direction or control over them "in carrying out the conduct."[262] Under Article 8, merely encouraging or expressing support for the acts of non-state actors will not constitute "control." The specific level of control by the state over the non-state actors to attribute those acts to the state, however, is debatable. Furthermore, the question of the level of control by the state over these acts that would be necessary to attribute those actions to the state to allow the use of force against the territory of the host state in self-defense is a hotly contested issue. The courts have provided some guidance, but it is not necessarily consistent or clear.[263]

---

[260] THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY INTRODUCTION, TEXT AND COMMENTARIES 99 (James Crawford ed., 2002); *see also* Responsibility of States for Internationally Wrongful Acts, *supra* note 256, art. 7.

[261] Responsibility of States for Internationally Wrongful Acts, *supra* note 256, art. 5, at 3.

[262] *Id.* art. 8.

[263] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 115 (June 27) (recognizing the "effective control" test); Prosecutor v. Tadić, Case No. IT-94-1-I, Judgment, para. 123 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (implying the presence of a test less exacting than "effective control" in defining the "overall control" test); TALLINN MANUAL, *supra* note 18 (manuscript r. 6, para 10).

In the *Nicaragua* case, while the court had concluded U.S. arming of the contras was not an armed attack for purposes of Article 51 of the U.N. Charter, it did find that the U.S. action violated its legal obligation not to "intervene in matters within the domestic jurisdiction of a State."[264] In other words, the United States had committed an internationally wrongful act in violation of a legal obligation and was therefore responsible for the harm done. The court explained that the principle of non-intervention prohibits acts of intervention against a state's free choice of a "political, economic, social and cultural system, and the formulation of foreign policy."[265]

The court noted that cases of intervention using force would be wrongful whether it is a "direct form of military action or in the indirect form of support for subversive or terrorist armed activities within another State."[266] The court made it clear that it is unlawful for one state to provide assistance for armed action by non-state groups against another state.[267] In finding that the United States had substantially supported the military operations of the contras, the court decided that the United States had acted "in breach of its obligations under customary international law not to use force against another State, not to intervene in its affairs."[268]

In the *Congo* case, the court provided additional analysis on the issue of the level of control by a state over the non-state actors' actions required to hold the state responsible for the actions of non-state actors. In this case, the court concluded that Uganda had given training and military support to an armed group operating against the Congolese government and held that this support constituted violations of the principles of non-use of force and non-intervention, even though the court did not find that Uganda controlled the operations of that group.[269] The court also found that the Congo was not in a position to end the groups' activities, and therefore the court said it could not conclude that the Congo had "tolerat[ed]" or "acquiesce[d]" in the groups'

---

[264] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, para 288 (quoting Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Order, 1984 I.C.J. 169, para. 41 (May 10)).

[265] *Id.* para 205.

[266] *Id.*

[267] *Id.* para 242.

[268] *Id.* para 292.

[269] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, paras. 160–63 (Dec. 19).

activities.[270] The court therefore did not uphold Uganda's claim against the Congo for tolerating the groups.[271]

Based on these decisions by the court, a state that provides military support or guidance to an armed group may be found guilty of committing "unlawful intervention" and possibly "unlawful use of force" even if it was not involved with planning and directing the operations of the group.[272] Furthermore, a state will be held responsible if it can prevent such groups from acting within its territory and fails to do so, but not if it is unable to do so.[273] This principle may be more difficult to apply in the context of cyber operations, however, where it may be difficult to determine whether the failure to stop such activities is the result of a state's unwillingness to deal with the problem, because it supports the cyber operations, or its inability to stop the operations, for example, because the state cannot convince the private sector entities such as the Internet Service Providers ("ISPs") to stop the malicious traffic causing the damage to the target. In sum, however, the principle reinforces the right of an attacked state to use force to protect itself from such attacks if it has no other remedy. How this may play out in the cyber domain, however, is debatable with little state practice to analyze to date.

The international courts have not had the occasion to rule on the application of existing law to cyber conflict. And it is likely that we will not see such decisions in the near future. While some may point to the accomplishments of the courts in other areas of the law of armed conflict, unfortunately, on some of the key questions related to use of force and state responsibility, the courts have provided mixed, and at times, confusing guidance. Certainly, one can conclude from the courts' opinions that they are not oriented to practical considerations that states must deal with and are therefore of more limited utility in the real world of armed conflict. Especially in the context of cyber, where clear, immediate evidence may be impossible to produce, states may be left to their own recourse in defending against cyber attacks from state and non-state actors. Ultimately, the decisions of the international courts will not take the place of international agreements or state practice as the primary sources of the law related to the use of force. However, these decisions still

---

[270] *Id.* paras. 300–01.

[271] *Id.*

[272] *See* Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHI. J. INT'L L. 83, 89–90 (2003).

[273] *Cf. id*.

provide important understanding of the consensus of at least some parts of the international community as to how these rules will apply.

2. Self-Defense: When Non-State Actors are Conducting Armed Attacks

In the cyber context where aggression from non-state actors can be of enormous consequence, as discussed in the previous Subpart, the ability of a state to hold non-state actors accountable and exercise its right of self-defense against the aggressor within the territory of another state will at times be deemed necessary. Yet the ability of a state to attribute responsibility of non-state actors to the state and then to use force in self-defense against the state has been controversial under international law.

Beyond the general legal responsibility that may be imposed upon a state for the actions of non-state actors, there remains the additional question of whether a state's support to non-state actors entitles the victim state to use force in self-defense. If so, can the state use force against the state itself or solely the non-state actors? The notion that actions by irregular forces can constitute armed attack is not contested by states. The issue of cross-border action by irregular forces has given rise to much difficulty in interpreting the law related to the use of force. If these forces are acting on behalf of the state from whose territory they are operating and their actions are of such gravity as to amount to an armed attack, the legal situation is clear.[274] However, the question of what degree of state involvement is necessary to allow the use of force against the territory of the host state in self-defense has proven to be a very complicated one under the law. Moreover, states have shown that they will act in self-defense against non-state actors conducting attacks against the state.[275] The controversy, however, is centered around the issue of how much state involvement in the non-state actor's actions is necessary to make those actions attributable to the state, justifying action in self-defense within the other state.

Since the terrorist attacks of 9/11, this question has been the focus of much discussion. Most recently, for example, in May 2011, the United States, without the consent of Pakistan, sent U.S. forces into Pakistan to capture or kill

---

[274] *See* Ian Brownlie, *International Law and the Activities of Armed Bands*, 7 INT'L & COMP. L.Q. 712, 731–33 (1958).

[275] *See, e.g.*, Jinks, *supra* note 272, at 83.

Osama bin Laden.[276] Following the operation, the Pakistani government objected to the U.S. action, arguing that it was an "unauthorized unilateral action."[277] President Obama had previously stated that, "if we have actionable intelligence against bin Laden or other key al-Qaeda officials . . . and Pakistan is unwilling or unable to strike against them, we should."[278] And in May 2010, the United States did.[279]

While commentators and academics have debated whether the U.S. operation in this case was lawful under international law, the United States has continued the use of the armed drones against individual terrorists in other states such as Yemen, Syria, and Pakistan. This indicates that the U.S. will continue to use force in self-defense against non-state actors even if they may reside in states against which the United States is not in armed conflict.[280] Codified international law, however, does not provide those states that are the victims of ongoing attacks by non-state actors sufficient guidance about the factual and legal standard to apply when determining whether to use force in self-defense under circumstances where a non-state actor is conducting armed attacks and may be receiving support from another state.

In the *Nicaragua* case, the court not only ruled on the illegal use of force by the United States but it also addressed the U.S. argument that its use of force was justified as collective self-defense of Costa Rica, Honduras, and El Salvador in response to armed attacks on those states by Nicaragua. The court rejected this argument finding that there was no armed attack by Nicaragua. According to the *Nicaragua* case, the assistance to rebels in the form of provisions of weapons or logistical or other support did not amount to an armed attack and therefore would not justify the use of force in self-defense by

---

276 Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483, 485 (2012).

277 Jane Perlez & David Rohde, *Pakistan Pushes Back Against U.S. Criticism on Bin Laden*, N.Y. TIMES, (May 3, 2011), http://www.nytimes.com/2011/05/04/world/asia/04pakistan.html.

278 Andy Merten, *Presidential Candidates Debate Pakistan*, MSNBC, (Feb. 28, 2008, 4:24 PM), http://www.msnbc.msn.com/id/23392577/ns/politics-decision_08/t/presidential-candidates-debate-pakistan.

279 *See id.*

280 *Is Osama bin Laden Killing Legal? Law Experts Divided*, INT'L BUS. TIMES (May 7, 2011, 8:39 AM), http://www.ibtimes.com/osama-bin-laden-killing-legal-international-law-experts-divided-282739; Joshua Norman, *Was the Killing of Osama bin Laden Legal?*, CBS NEWS (May 3, 2011), http://www.cbsnews.com/8301-503543_162-20059382-503543/was-the-killing-of-osama-bin-laden-legal-/; See recent testimony at his confirmations hearings by John Brennan, President Obama's nominee for CIA Director, discussing the administration's use of drone strikes on a U.S. citizen. *Open Hearing on the Nomination of John. O. Brennan To Be Director of the Central Intelligence Agency Before the S. Select Comm. On Intelligence*, 113th Cong. (2013), at 122–25 (pre-published hearing transcript *available at* http://intelligence.senate.gov/130207/transcript.pdf).

the victim state.[281] However, the court also ruled that while this type of assistance to the rebels would not amount to an armed attack, it could be illegal intervention or an illegal use of force.[282] In establishing a high threshold for what may constitute an armed attack, in contrast to an illegal intervention or use of force, the court ruled that both Nicaragua and the United States had not committed an armed attack by assisting irregular forces. The court did find, however, that the "sending" of armed rebel groups or "substantial involvement" in their attacks would justify the use of force in self-defense.[283]

In the *Nicaragua* case, the court treated the *Definition of Aggression* with its provision "sending by or on behalf of a state or its substantial involvement therein" as definitive as to what amounted to an armed attack. According to the *Nicaragua* court, the United States would be held responsible for the actions of the irregular armed groups if it had "effective control" of the specific operations in question.[284] In contrast, the United States would not be held responsible for the actions of the contra forces, according to the court, merely because it had a "preponderant or decisive" control over their operations in general. The court did not rule on whether any lesser level of state involvement, such as acquiescence or an inability to control armed bands operating in its territory, could be enough to constitute an armed attack. Rather, the court held that only if it could be shown that the United States "had effective control of the military or paramilitary operations in the course of which the alleged violations were committed" could the United States be held responsible for the actions of those groups.[285]

One implication of the court's ruling is that as long as the supporting state refrains from controlling the group's specific actions, it will be free from a self-defense use of force action from the victim state. While the supporting state would still be responsible for its actions, and the victim state would be able to seek reparations or other remedies from the other state, according to the court's ruling, the victim state would be prohibited from lawfully acting in self-defense and using force. The legal framework provided by the court will

---

[281] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 247 (June 27).
[282] *Id.* para. 195.
[283] *Id*. para. 195.
[284] *Id*. para. 115.
[285] *Id.*

likely fail to act as any deterrent for aggressor states using non-state actors as proxies in cyber operations, as the Chinese have been reported to be doing.[286]

After the court's decision in the *Nicaragua* case, the U.N. International Law Commission adopted the Articles on State Responsibility, which argued that a state would be responsible for the acts of "organs of a State" or of "persons or entities exercising elements of governmental authority," as well as "conduct directed or controlled by a State."[287] Later on in the *Armed Activities on the Territory of the Congo Case*, the court applied this test and found that the Court had not received "probative evidence that Uganda controlled, or could control, the manner in which [the Congo Liberation Movement] put such assistance to use."[288] One positive implication from the court's decision is that attacks by armed bands or irregulars directly or indirectly supported by a state gives rise to a right of defense against that state.[289] However, another implication is that the court may not recognize any right of defense against attacks from rebel groups operating from the territory of a state where that state is not directly or indirectly involved with the attacks.[290]

The court leaves unanswered the question whether the court intended to prohibit targeting the state itself when the state is not involved or unable to stop the attacks, or whether the court meant to prohibit more broadly any action within the other state in response to the attacks. If the latter, the court's decision would significantly limit a state's right of self-defense under the U.N. Charter. Particularly in the cyber context, such an interpretation would leave victim states at a significant disadvantage against those states that carry out aggressive cyber attacks through either state-owned entities or private hackivists.

As international courts have developed, there has been little difference in the substantive legal decisions of the different courts. With respect to the issues related to non-state actors and state responsibility, however, the ICJ and the ICTY did differ on one substantive legal point that has particular significance in the context of armed conflict. The difference related to the test for

---

286 Thomas, *supra* note 110, at 101.

287 Responsibility of States for Internationally Wrongful Acts, *supra* note 256, arts. 5, 8.

288 Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, para. 16 (Dec. 19).

289 *See id.* paras. 134, 144–47.

290 *Id.* para. 146 ("The Court has found . . . . .that there is no satisfactory proof of the involvement in these attacks, direct or indirect, of the Government of the DRC. . . . [E]ven if this series of deplorable attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC.").

determining the responsibility of a state or its officials for actions taken by a non-state entity over which the state exercised significant influence or control. Under the *Nicaragua* standard, as mentioned above, a state cannot be held responsible for the actions of a non-state actor merely because it had general control over their operations. Rather, the court held in that case that the United States could only be held responsible under circumstances where it was proved that the United States had "effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[291]

In contrast, in 1999, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia concluded in the *Tadić* case that the *Nicaragua* test of "effective control" was "at variance with judicial and State practice," and instead decided that:

> In order to attribute the acts of a military or paramilitary group to a State, it must be proved that the State wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity. . . . However, it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law.[292]

The *Tadić* court ruled that the Federal Republic of Yugoslavia ("FRY") did exercise the required overall control over the Bosian Serb Army "in terms of participation in the general direction, coordination and supervision of the activities and operations" of that Army.[293] In this case, the ICTY determined that in order to bring responsibility to the State of Yugoslavia based on the actions of the Bosian Serbs, there was not any need to "prove that each operation during which acts were committed in breach of international law was carried out on the FRY's instructions, or under its effective control."[294] In this case of finding criminal liability for the accused, the ICTY found that a lesser standard of attribution of state complicity in the acts of the non-state actor could be used in order to hold the state responsible.

---

[291] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, para. 115.

[292] Prosecutor v. Tadić, Case No. IT-94-1-I, Judgment, para 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

[293] *Id.* paras. 147, 156.

[294] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bos. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 402 (Feb. 26).

Some scholars have pointed out that the courts have appeared to develop two different standards by which to assess attribution from non-state actors to the state.[295] Under the *Nicaragua* court standard, a state is responsible for the acts of non-state actors where it has "effective control" over the actors.[296] Under this standard as applied in the context of cyber activities, the provision of cyber expertise or training, alone, by the state to the non-state actor in the planning of specific cyber attacks against another state would likely not be enough to give rise to state responsibility for the wrongful acts committed by the non-state actor.[297] In contrast, under the *Tadić* standard, as some scholars have pointed out,[298] the ICTY created a lower threshold of "overall control" in the context of individual criminal responsibility and for determining the nature of the armed conflict.[299] If the *Tadić* standard were applicable within the cyber context where states are actively funding cyber attacks against U.S. computer systems and providing money and political cover for young hackers trained to attack these computer networks, it is likely that with the lower threshold applied, the states would be found responsible for the hackers' actions.

This position that there exists two different standards for determining state responsibility has been challenged by the court in the *Genocide* case. In 2007, the ICJ in the *Genocide* case ruled on the issue of the degree to which Serbia could be held responsible for actions by Bosnian Serb forces.[300] In reviewing the previous decision by the ICTY in the *Tadić* case, the ICJ ruled that the "overall control" test applied in the *Tadić* case was suitable for the *Tadić* court to invoke since it was ruling on whether the FRY involvement was so substantial as to rule the conflict in Bosnia as international in character.[301] The ICJ noted that the application of the "overall control" standard by the ICTY in a case determining criminal liability of individuals and assessing the international nature of the conflict was appropriate. But the ICJ drew a

---

[295] *See, e.g.*, Stefan Talmon. *The Responsibility of Outside Powers for Acts of Secessionist Entities*, 58 INT'L & COMP. L.Q. 493, 497 (2009).

[296] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, paras. 105, 109; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 2007 I.C.J. 43, para. 404.

[297] TALLINN MANUAL, *supra* note 18 (manuscript r. 6, para. 10).

[298] Jinks, *supra* note 272, at 89.

[299] Prosecutor v. Tadić, Case No. IT-94-1-I, Judgment, paras. 122, 124 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

[300] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 2007 I.C.J. 43, paras. 403–04.

[301] *Id.* para. 404 ("Insofar as the 'overall control' test is employed to determine whether or not an armed conflict is international, which was the sole question which the Appeals Chamber was called upon to decide [in *Tadić*], it may well be that the test is applicable and suitable . . . .").

distinction based upon the different jurisdictions of the courts and found that applying the same "overall control" test in a case dealing with state responsibility under international law, the *Genocide* case, would be "unpersuasive."[302]

The ICJ concluded that the "overall control" test—the lower threshold—was unsuitable for determining state responsibility for wrongful actions of non-state actors "for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a state's organs and its international responsibility."[303] The court went on to rule that the FRY was not responsible for specific violations committed by these entities, notwithstanding the considerable influence and control that the FRY exercised over them.[304] Even if the overall control test were applied, the required control by the state would need to go beyond "the mere financing and equipping of such forces and involv[e] also participation in the planning and supervision of military operations."[305]

One negative implication of the courts' different interpretations of standards is that states are given the opportunity to carry out criminal policies through non-state actors while escaping from direct responsibility.[306] As the Vice-President of the Court, Judge Al-Khasawneh noted in his dissent:

> When . . . the shared objective is the commission of international crimes, to require both control over the non-State actors and the specific operations in the context of which international crimes were committed is too high a threshold. The inherent danger in such an approach is that it gives States the opportunity to carry out criminal policies through non-state actors or surrogates without incurring direct responsibility therefore.[307]

For criminal purposes the court has indicated that the lower level of control will be used (the overall control test) but, for assessing state responsibility, the

---

[302] *Id.*

[303] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 2007 I.C.J. 43, para. 406.

[304] *Id.* paras. 368–69.

[305] *Tadić*, Case No. IT-94-1-I, para. 145 ("[W]ith regard to . . . individuals or groups [not organized into military structures], courts have not considered an overall or general level of control to be sufficient, but have instead insisted upon specific instructions or directives aimed at the commission of specific acts, or have required public approval of those acts following their commission.").

[306] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 2007 I.C.J. 43, para. 39 (Vice-President Al-Khasawneh, dissenting).

[307] *Id.*

higher threshold will be used (the effective control test).[308] The higher threshold will likely allow states to avoid being held responsible for actions that non-state actors have taken on their behalf. Another implication of the courts decisions will be to make it difficult for states as well as non-state actors, to understand the relevant standards related to state responsibility and to act within the legal boundaries.[309] This poses difficulty for decisions-makers who are trying to comply with the law. Certainly, the principle of state responsibility should not require a state to intervene to prevent all violations by other entities just because it has the capability to do so. However, a state should have some responsibility to act where attacks are being carried out against other states by an entity over which it exercises overall control and provides essential support.

When a state knows or has reason to know that entities under its overall control are carrying out harmful and illegal actions against another state, or are likely to, that state should have the responsibility to take reasonable actions to prevent or terminate those actions. It should not be up to that state to deny all responsibility simply because it did not order or control the specific operation in which the violation occurred. To find otherwise would effectively overrule a state's obligation recognized under customary international law to do no harm to others.[310] The critical question is what would constitute reasonable actions by the state. The standard provided at the end of this Article seeks to address this issue.

In the ICJ's *Genocide* decision there is one potentially useful standard that the court employed related to the question of the FRY's responsibility for acts of genocide committed by other individuals and entities to which it gave considerable support and over which it exercised considerable influence.[311] Although the court had previously asserted that states could only be held responsible for acts by other entities if the actions were "in accordance with the States' instructions or under its 'effective control,'"[312] on the issue of genocide the court accepted a lower standard for holding state responsible for acts of genocide under the Genocide Convention.[313] With respect to the obligation "to

---

[308] *See id.* paras. 396–407 (Judgment).

[309] *Cf.* TALLINN MANUAL, *supra* note 18 (manuscript r. 6, para. 10).

[310] For further discussion on the standards of state responsibility, see Cassese, *supra* note 164, at 656–57.

[311] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 2007 I.C.J. 43, para. 400.

[312] *Id.*

[313] *Id.*

prevent" genocide, the court adopted a different standard for state responsibility.[314] Under this standard, the court ruled:

> [R]esponsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance.[315]

In assessing whether a state has carried out its obligation to prevent genocide, the Court provided the following criteria: (1) the capacity of the state to influence effectively the action of persons likely to commit genocide, (2) the geographic distance of the state from the scene of the events, and (3) the strength of the political links, as well as other links, between the authorities of the state and the main actors in the events.[316] Ultimately, the court found that the FRY had failed in its duty to prevent the massacre at Srebrenica. The court concluded:

> [T]he FRY was in a position of influence over the Bosnian Serbs who devised and implemented the genocide in Srebrenica . . . owing to the strength of the political, military and financial links between the FRY on the one hand and the [Bosnian Serb entities] of the other . . . . [T]he Belgrade authorities . . . could hardly have been unaware of the serious risk.[317]

The court noted, however, that a state's "capacity to influence" must also be assessed by the legal limits the state is obligated to follow under international law in taking any action.[318] Although the court did not explain what it meant by this, it seems to imply that a state may not use force against another state to prevent genocide if such use of force would otherwise be unlawful. Although this case dealt with obligations of a state to prevent genocide, the criteria developed by the court will be useful in assessing whether a state has done enough to prevent cyber attacks from emanating from its state and harming another state.

For the purposes of attribution for state responsibility, it may be that initially limited, available evidence will not allow a clear "control" link to be made between the state and the non-state actors. In cyberspace, particularly

---

314 *Id.* para. 430.
315 *Id.*
316 *Id.*
317 *Id.* paras. 434, 436.
318 *Id.* para. 430.

where a state may respond in self-defense, even acknowledging publicly that it is doing so, under the court's rulings the victim state may be held responsible for an act of aggression unless the state is able to show proof that the state is acting in response to armed attacks by the state.[319] Especially in cyberspace where the ability to identify the attacker with certainty will be difficult if not impossible, without a consensus on the rules related to state responsibility, states may be left with the choice of either doing nothing (likely not to happen if the state has suffered severe cyber attacks) or taking action in self-defense and risking a court or the international community finding that the state violated international law.

If evidence is not readily available at the time of the attacks, however, it is possible for the victim state to use information gathered after the attacks in order to make a case for the right to use force in self-defense. The court in the *Diplomatic Hostages* case indicated that acts may be attributed to the state retroactively.[320] In November 1979, a group of Islamist students and militants took over the American embassy in Tehran and held fifty-two Americans hostage for 444 days.[321] Although originally the state had not directed or been involved with the attack against the U.S. embassy, Ayatollah Khomeini had supported what the group was doing.[322]

The court found that the state was responsible for the actions of the group that was holding the hostages and held that the state was required to stop the students.[323] After the fact, if a state provides approval and support helping to perpetuate the unlawful acts of a non-state actor within it territory, that state can be held responsible for those actions even if the state did not originally direct them.[324]

Even accepting that there may exist a right of self-defense against non-state actors, there exists a debate under international law about the extent of a victim state's right of self-defense against these actors that reside in the territory of another state. For instance, in the *Corfu Channel* case the court attributed

---

319 *See* Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 71 (Nov. 6) (holding that the U.S. defense was insufficient because the US had failed to provide "conclusive" proof of its allegations against Iran, even though it had presented "highly suggestive" evidence).

320 United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3 (May 24).

321 Mike Bagully, *The Iranian Dilemma*, GEO. PUB. POL'Y REV., WINTER 2005–2006, at 111, 112.

322 *United States Diplomatic and Consular Staff in Tehran*, 1980 I.C.J. 3, para. 59.

323 *Id.* paras. 67–68.

324 *See id.* para. 69–70.

actions related to the laying of the mines to Albania since it "should have known" about the mines,[325] and the Court found that Albania violated its duty not to allow its territory to be used to harm another state.[326] The court, however, also significantly limited the victim state's right of self-defense by finding that Great Britain violated the sovereignty of Albania by sweeping for mines in the Channel without Albania's consent.[327] International legal scholars have argued that the court, in limiting Great Britain's right of self-defense to sweep the mines and use force necessary to promptly end the illegal attacks against shipping, undermined the legal norms of the U.N. Charter against aggression.[328] It may be that in ruling in this manner, the court also undermined its own authority since states will not silently accept aggressive attacks.

In the *Congo* case, the Democratic Republic of the Congo ("DRC" or "the Congo"), brought an action against Uganda for unlawful use of force within the Congo.[329] Uganda, however, claimed that it was using force in self-defense against armed attacks by non-state actors, the irregular forces of the Allied Democratic Forces, from the territory of the DRC in the period from August 1998 till June 2003. Uganda argued it had the right of self-defense against irregular armed forces and Congolese-government supported forces because they were attacking into Uganda from the Congo.[330] The Congo claimed that the attacks were the actions of an independent, non-state military force, the Allied Democratic Forces.[331] Uganda argued that the Allied Democratic Forces were supported by the Congo.[332] The court accepted arguments made by the Congo when it denied that it had any role in the attacks.[333]

The court, in following the same approach as the *Nicaragua* court, found there was a lack of evidence provided by Uganda that would show that the DRC was supporting the groups that were attacking Uganda. In invoking the Definition of Aggression Article 3(g), it concluded that on the evidence before

---

325 Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 18 (Apr. 9).

326 *Id.* at 22–23.

327 *Id.* at 35.

328 *E.g.*, Moore, *supra* note 228, at 918.

329 Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 107–09 (Dec. 19).

330 *Id.* para. 131.

331 *Id.* para. 133 ("The DRC does not deny that a number of attacks took place, but its position is that the [Allied Democratic Forces] alone was responsible for them.").

332 *Id.*

333 *Id.* paras. 146–47.

it the attacks were not attributable to the DRC. Therefore, the court found that Uganda did not have the right of self-defense against the DRC.[334] The court in its decision, however, expressly avoided the questions whether there may be an armed attack by non-state actors in the absence of state involvement, and what measures a state may take against such an attack.[335] The decision of the court *implied* that attacks by bands or irregulars directly or indirectly supported by a state could give rise to a right of defense against the state.[336] Unfortunately, the court left unanswered whether there is any right of self-defense against attacks from rebel groups operating from the territory of a state where the state is neither directly nor indirectly involved with the attacks. The court found "no satisfactory proof of the involvement in these attacks, direct or indirect, of the Government of the DRC. The attacks did not emanate from armed bands or irregulars *sent by* the DRC or on behalf of the DRC . . . ."[337]

This passage from the case suggests that the court does not recognize a right of the victim state to use force against a state from whose territory an armed group is conducting attacks if that state had not "sent" the groups or was not "involved" in the attacks in question. The implication from the *Congo* decision is that it would be illegal to target the state *itself* when that state is not involved with any insurgent attacks from its territory and is unable to end those attacks. For example, in the cyber context, responsive distributed denial of service ("DDOS")[338] attacks against a state's networks would not be appropriate unless there was evidence that the state sponsored the attacks by the non-state actors. The question left unanswered by the court, however, is whether the victim state can target the non-state actors responsible for the attacks (not the state itself) within the other state's territory.

The *Congo* decision ought not stand for the proposition that victim states have *no* right of response under self-defense on the territory of another state (from which the attacks are coming) against the groups operating from the territory of that state. For example, a state ought to be allowed to use cyber tools to take down the networks in the target state used by the individuals carrying out the cyber attacks against the victim state. The victim state would

334 *Id.* para 147.

335 *Id.*

336 *See id*. paras. 130–47.

337 *Id.* para. 146 (emphasis added).

338 A distributed denial of service is an attack which "attempt[s] to prevent the legitimate use of a service," such as the Internet. *See* Jelena Mirkovic & Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, COMPUTER COMM. REV., April 2004, at 39, 40.

be taking those networks down in order to stop the threat coming from those networks. The language of Article 51 of the U.N. Charter does not distinguish between armed attacks conducted by a state from ones conducted by non-state actors.[339] Also, the U.N. Security Council resolutions after 9/11 clearly preserved the right of self-defense against a non-state actor under Article 51.[340]

In a case the year before the *Congo* decision, the court provided an advisory opinion on the legality of the wall that Israel had begun constructing in 2002 to cordon off the West Bank in response to an ongoing wave of terrorist attacks.[341] Like in the *Congo* case, the court avoided any specific ruling on the possibility of self-defense against an armed attack by non-state actors. However, in its opinion, the court gave only a very brief discussion of self-defense, such that some have interpreted the court's ruling as a rejection of any doctrine of self-defense against an armed attack by non-state actors.[342]

The issue before the court was whether Israel had the right of self-defense to create the wall to prevent the ongoing terrorist attacks against it. In its opinion, the court stated:

> Article 51 of the Charter . . . recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign State. . . . Consequently, the Court concludes that Article 51 of the Charter has no relevance in this case.[343]

The court reached its conclusion finding against any right of self-defense for Israel because the alleged aggressor was not a state.[344] As far as Article 51 was concerned, according to the court, a non-state actor could not conduct an "armed attack" as defined in Article 51.[345] Although nothing in the language of Article 51 indicates such a limitation, the implication of the court's ruling on

---

339 *See* U.N. Charter art. 51.

340 S.C. Res. 1368, *supra* note 156.

341 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

342 Sean D. Murphy, *Self-Defense and the Israeli* Wall *Advisory Opinion: An* Ipse Dixit *from the ICJ?*, 99 AM. J. INT'L L. 62, 63 (2005); Ruth Wedgwood, *The ICJ Advisory Opinion on the Israeli Security Fence and the Limits of Self-Defense*, 99 AM. J. INT'L L. 52, 58 (2005).

343 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004 I.C.J. 136, para. 139.

344 *Id.*

345 *Id.*

this was that there is no right of defense against aggression perpetrated by non-state actors.

The court cited no legal authority for its restrictive reading of the U.N. Charter's right of self-defense. Nor did the court recognize that its decision was at odds with a series of U.N. Security Council resolutions in response to the 9/11 attacks.[346] As discussed previously, on September 12, 2001, the Security Council unanimously passed Resolution 1368, condemning the attacks and invoking the right of self-defense in calling on the international community to combat terrorism.[347] The resolution does not limit its application to terrorist attacks by state actors only. In the days following the U.S. invasion of Afghanistan, the U.N. Security Council condemned the Taliban regime "for allowing Afghanistan to be used as a base for the export of terrorism by the Al-Qaida network . . . ."[348] In U.N. Security Council Resolution 1373, the Council made it clear that "international terrorism[] constitute[s] a threat to international peace and security"[349] while "[r]eaffirming the inherent right of individual or collective self-defence as recognized by the Charter of the United Nations . . . ."[350]

Without evidence of direct Taliban support or control over al Qaeda, the U.N. Security Council passed resolutions 1368 and 1373 invoking the principle of self-defense under Article 51 and supporting the legal authority of a victim state to use force in the sovereign territory of another state because of the actions of a non-state actor within that state.[351] The ICJ's opinion seems to ignore the Security Council's position on this point. Arguably, the Security Council, whose resolutions are legally binding and whose membership represents the membership of the United Nations, ought to hold greater weight in its legal pronouncements, compared to an advisory opinion by the ICJ, which is not legally binding under international law.

It would be difficult to imagine that a state that has been attacked by a non-state actor would not invoke its right to respond in self-defense against the attackers, no matter where they may be if the state from which they were attacking refused or was unable to do anything to stop the attackers. In the

---

346 *See supra* note 197; *see also* S.C. Res. 1377, U.N. Doc. S/RES/1377 (Nov. 12, 2001); S.C. Res. 1373, *supra* note 68.

347 S.C. Res. 1368, *supra* note 156.

348 S.C. Res. 1378 pmbl., *supra* note 166.

349 S.C. Res. 1373, *supra* note 68, pmbl.

350 *Id.*

351 *Id.*; S.C. Res. 1368, *supra* note 156.

cyber context, imagine that a critical infrastructure like the water supply of a state has been compromised by a cyber attack, leaving the state without water supply to its population or with contaminated water. With the looming threat of loss of life, irreparable harm to its population, and further cyber attacks, the victim state would need to act expeditiously to stop the damage, including using force within the territory of the state from which the malicious code emanated from.

If the state from which the cyber attack emanated is unwilling or unable to carry out its responsibility to prevent its territory from being used as a base for cyber attacks against other states, there is a right of individual and collective defense on the part of the attacked state against the source of the aggression. If, however, the state whose territory the aggressors are operating from is directly or indirectly involved in supporting the attacks, then the state itself can be a legal target of the victim state. Arguably, even if there is no involvement between the state and the aggressors operating within the state, the victim state has the right to exercise its right of defense against the aggressors themselves. To argue otherwise would in effect mean that the right of self-defense is meaningless.

3. Requirements of Necessity and Proportionality Under Self-Defense

If a victim state was to use force against those conducting the attacks from within another state, it would have to follow the requirements of necessity and proportionality. Although these principles are not codified within the U.N. Charter, they are considered part of customary international law.[352] state practice has shown that the principles of necessity and proportionality have played a central role in state justification of the use of force in self-defense and in international responses to attacks. These principles of self-defense under international law also apply in the cyber domain for a state operating in self-defense.[353]

The "necessity" requirement of *jus ad bellum* is a prohibition against the use of force except when the victim state determines that non-forcible measures would not effectively stop the threat. In other words, there was no

---

[352] *E.g.*, Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, para. 147 (Dec. 19) (noting that military action against airports and towns was a disproportionate response to cross-border attacks); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 324, para. 43 (Nov. 6); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 41 (July 8); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 194 (June 27).

[353] TALLINN MANUAL, *supra* note 18 (manuscript rr. 14, 15).

other means to resolve the dilemma but by using force. If, for example, a victim state was to use force in self-defense within the territory of another state where the non-state actors were launching attacks, necessity requires that the state contemplating the use of force first assess whether non-forcible remedies such as diplomatic intervention with the state would stop the attacks or prevent future attacks. If through diplomatic discussions the state takes steps such as arresting those responsible for the attacks, thereby removing the threat, the victim state would no longer have a legal right to use force since it was no longer necessary to use force to stop the attacks. For example, in assessing whether Iran may have had a legal right to use force in self-defense against the state or states responsible for targeting its uranium facility with the Stuxnet worm, assuming a state was responsible, Iran would have no right of self-defense once the cyber attack stopped and the threat of attacks no longer existed. If the victim state did use force after the attacks were over and the threat was no longer, it would likely be an act of reprisal and illegal under international law. If an attack is imminent, however, the circumstances may be that there is no time to pursue other measures and the victim state acts necessarily, invoking its right of self-defense.

To avoid the appearance of a self-defense response being an act of reprisal, especially if the attacks appear to be complete with little evidence of their continuation, the victim state should formally complain to the state from which the attacks came from before using force. Before using any force in self-defense, the victim state ought to complain to the state, notifying the state of the attacks and giving the state the opportunity to stop the cyber attacks from its territory. In complaining to the state about the threat the victim state will likely be able to rebut any argument that its actions in self-defense, if it ultimately resorts to force, were reprisals and seemingly unnecessary.[354] Although there is no such mandatory requirement for all self-defense responses under international law, the ICJ has found against United States' use of force in self-defense where the United States failed to complain to the state about the threat. The court reasoned that the lack of a complaint was evidence that the use of force against the target was not necessary.[355]

---

[354] *Oil Platforms*, 2003 I.C.J. 324, paras. 73–76. In the Oil Platform case the court was not satisfied that the attacks on the platforms were necessary to respond to these incidents. The court said it found no evidence that the U.S had complained to Iran of the military activities of the platforms, which, the court suggested, meant that the targeting of the platforms was not seen as a necessary act. *Id.*

[355] Taft, *supra* note 244 (arguing that the court's statement related to the U.S. not complaining to Iran about the threats from the platforms was too restrictive under the principle of self-defense and without basis in international law and practice.).

In the case where an armed attack has already occurred, and the attacks are ongoing or the victim state believes that future attacks will occur, the criteria of the *Caroline* incident for invoking anticipatory self-defense does not need to be applied. Under this criteria, for the right to forcibly respond in anticipation of an attack a state needs to show "*necessity* of self-defence, instant, overwhelming, leaving no choice of means and no moment for deliberation."[356] The element of the standard requiring imminence, however, ought not be applied to a response to an attack that has already occurred. In fact, if the state believes that the attacks will continue, the state has the authority to act immediately in order to prevent further attacks as long as it can attribute the cause of the attack and its response is proportionate.

It follows then that when acting under Article 51 self-defense authority, if an actual armed attack has already taken place, the imminent criteria of necessity would be moot. A victim state that suffered a devastating attack would likely not deliberate long if at all about alternative measures as long as it was certain about attribution and the likelihood of future attacks. In the cyber domain, where the threats from malicious computer code arise at lightning speed, the victim state may have no other choice but to respond immediately in order to stop further damage. The state would still be required to respond, however, with proportionate force to deter the threats.

Proportionality under *jus ad bellum* requires that any forcible response in self-defense be limited in size and magnitude to what is reasonably necessary to achieve the permissible objectives of the self-defense operation.[357] Proportionality relates to the size, duration and target of the response. Only that force that is necessary to stop the threat can be used and nothing beyond what is required. The self-defensive measures are to be used to halt and/or repel the attacks and not to act in a retaliatory or punitive manner.[358]

---

[356] Letter from Lord Ashburton, British Special Representative to the U.S., to Daniel Webster, U.S. Sec'y of State (July 28, 1842), *reprinted in* 30 BRIT. & FOREIGN ST. PAPERS 195, 198 (1858) [hereinafter Caroline Letters] (emphasis added) (internal quotation marks omitted) (quoting Letter from Daniel Webster, U.S. Sec'y of State, to Henry S. Fox, British Minister in Washington (Apr. 24, 1841), *reprinted in* 29 BRIT. & FOREIGN ST. PAPERS 1129, 1138 (1857)).

[357] *See* DINSTEIN, *supra* note 182, 262–67; *see also* MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, THE INTERNATIONAL LAW OF WAR: TRANSNATIONAL COERCION AND WORLD PUBLIC ORDER 242 (1994); JOHN NORTON MOORE, CRISIS IN THE GULF: ENFORCING THE RULE OF LAW 158 (1992).

[358] Declaration on Friendly Relations, *supra* note 136, Annex at 122; Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, *supra* note 136, at 12. In both resolutions, the General Assembly made it clear that reprisals are unlawful). *See also* S.C. Res. 188, para. 1, U.N. Doc. S/RES/5650 (Apr. 9, 1964) (condemning reprisals as unlawful).

Compliance with this requirement will depend on the factual situation as it was known at the time by the victim state.

Proportionality does not require the use of an equivalent level of force in a self-defense response. Nor does it require the use of the same types of weapons, the same number of armed forces, or that the actions be in the victim state's own territory.[359] Recently, the U.S. government has stated that if it suffers a cyber attack, the consequences of which would be equivalent to an armed attack in conventional combat, it would reserve the right to respond in self-defense to the cyber attack, including with kinetic force.[360] As long as the kinetic force used in response was only to the level that was necessary to stop or prevent other attacks and there were no other non-forcible measures that could be used to stop the attacks, the response would be proportionate and legal.[361]

Furthermore, a state that has suffered a cyber attack equivalent to an armed attack can use force electronically outside its territory through cyberspace against the attacker as long as non-forcible measures are not available to stop the threat. If, for example, "passive defense" security measures, non-forcible in nature, such as system access controls, data access controls, security administration, or secure system designs related to the victim's own networks, could be implemented to stop or prevent other cyber attacks, the principle of necessity would prohibit the victim state from using any forcible cyber measures against the attacker. However, if passive defenses are not available or would be ineffective in stopping or preventing the attacks, the victim state could use forcible measures—cyber "active defenses," such as electronically sending destructive viruses to the attacker's computer—as long as the use of the active defenses were proportionate to the threat from the adversary.[362]

According to some commentators, what matters in assessing proportionate actions is "the result to be achieved by the 'defensive' action, and not the

---

359 GRAY, *supra* note 188, at 150–55.

360 CYBERSPACE POLICY REPORT, *supra* note 2.

361 *See* Taft, *supra* note 244, at 305–06 (arguing that "[t]here is no requirement . . . that a State exercising the right of self-defense must use the same degree or type of force used by the attacking State in its most recent attack" and that, instead, "the proportionality of the measures . . . is to be judged according to the nature of the *threat* being addressed).

362 Active defenses in cyber could involve the sending of destructive viruses to the adversary's computer, manually or automatically, or packet-flooding the adversary's machine. The malware used can be designed to shut down, damage or destroy the adversary's computer networks, which would prevent the adversary from using those systems for future cyber attacks. *See generally* Matthew J. Sklerov, *Responding to International Cyber Attacks as Acts of War*, *in* INSIDE CYBER WARFARE *supra* note 43, at 45–76.

forms, substance and strength of the action itself."[363] However, there is agreement among commentators that there is only one legitimate goal for any self-defense response: to stop or prevent an attack. Any response that creates the impression that the action was intended to punish, embarrass or teach some broader lessen rather than to stop or prevent an attack, will be viewed as disproportionate.[364] Therefore, the size, duration and target of the response all become relevant factors in making an assessment on proportionate actions under the circumstances.

In the case of a state using force in response to attacks from non-state actors in another state's territory, proportionality might require special measures be taken into consideration when determining the appropriate target. For example, in cases where there is uncertainty regarding the state's complicity in the non-state actors attacks, the victim state should limit its attacks to the non-state actors and avoid or minimize the damage to the state's population and resources. Targeting the specific perpetrators of the attacks versus the state's assets or population would likely meet the proportionality test. In cyberspace this may entail avoiding the use force against state owned cyber assets or networks but seeking to use force against the specific computers, networks, assets of the attackers.

In August 1998, the United States responded to al Qaeda's attacks on its embassies in Kenya and Tanzania with missile attacks on the terrorist training camps in Afghanistan and a pharmaceutical plant in Sudan. The United States reported its actions to the Security Council under Article 51. The United States stated that the attacks were carried out to prevent and deter future attacks and after repeated efforts to convince Sudan and the Taliban regime in Afghanistan to shut down the terrorist facilities. The targets struck and the timing and methods of attack used were designed to comply with the rules of international law including the rules of necessity and proportionality.[365] There was no action taken against the United States at the Security Council and response from the

---

[363] Roberto Ago, *Addendum to the Eighth Report on State Responsibility*, U.N. Doc. A/CN.4/318/Add.5–7 (1980), *reprinted in* 1980 Y.B. INT'L L. COMM'N 13, 69, U.N. Doc. A/CN.4/SER.A/1980/Add.1.

[364] Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 74 (Nov. 6). Some judges in the Oil Platform case found the U.S. action to be unlawful reprisals, arguing that they were not necessary and proportionate. Judge Simma found that the U.S. actions were to teach Iran a broader lesson. *Id.* para. 15 (separate opinion of Judge Simma). Judge Kooijmans found that the U.S. actions were punitive. *Id*. paras. 52, 55, 62 (separate opinion of Judge Kooijmans).

[365] *See* U.N. Security Council, Letter dated 20 August 1988 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, U.N. Doc. S/1998/780 (Aug. 20, 1988).

international community was muted. Some writers, however, objected, raising questions about the necessity of the U.S. response, arguing that U.S. action was not necessary since the attacks against the U.S. nationals were over at the time the United States responded.[366]

In cyber operations, the deployment of computer code in self-defense targeted to stop an attack may pose a challenge when it comes to anticipating the second and third order effects of an act of self-defense. If in deploying malware in self-defense it is difficult to anticipate the possible consequences of the use of the code, compliance with the principle of proportionality may be complicated. For purposes of this discussion, assume that the Stuxnet worm was used in self-defense against Iran. In considering the factors size, duration, and target of the response of the Stuxnet worm, some of the challenges of proportional responses in cyber come to light. Critics of the Stuxnet cyber operation against Iran noted that the code was inadvertently released on the Internet, infecting many computers that were not the intended target.[367] Aside from raising possible concerns about the necessity of the Stuxnet action this illustration raises issues related to the proportionality of the response.

V. EFFECTIVE RESPONSES: STRENGTHENING NORMS OF STATE RESPONSIBILITY

In the case of a major cyber attack that causes destruction to a state's critical infrastructure, it is possible that the United States or any other country that has been targeted would want to respond. This could be either through diplomatic, economic, law enforcement, or, in very serious cases that reach the level of an armed attack, military action. Prior to 9/11, U.S. counterterrorism policy was based on law enforcement measures to prevent terrorist attacks.[368] This law enforcement-lead approach proved ineffective in stopping attacks against the United States. It may be the case that under certain circumstances

366 GRAY, *supra* note 188, at 197–98 (arguing that the U.S. response appeared to be reprisals meant to deter the terrorists and therefore in violation of the necessity requirement).

367 Although the U.S. government is suspected of launching the Stuxnet worm with the Israeli government, no government has taken credit for the operation so there is no evidence that a state is arguing a self-defense justification for the use of Stuxnet against Iran's uranium enrichment facilities.

368 *The State of Intelligence Reform Ten Years After 9/11: Hearing Before the H. Perm. Select Comm. on Intel.*, 112th Cong. (2011) ("Prior to the 9/11 attacks, the FBI's operations were heavily weighted towards its law enforcement mission; intelligence tools and authorities were primarily used for the counterintelligence mission. In the immediate aftermath of 9/11, the FBI quickly identified the need to enhance intelligence programs with improved analytical and information sharing capacities to detect and prevent future terrorist attacks.").

of a cyber attack against a state, the target state may determine that a military response would be necessary. This would be more likely when other efforts such as law enforcement measures have been deemed ineffective. While international law has recognized that non-state actors globally have the capacity to use catastrophic force that causes harm to states,[369] in many ways, the Internet has increased the potential that non-state actors could cause such harm.[370]

Just as some states support, tolerate, or harbor terrorists, there will likely be states that obstruct efforts to suppress cyber attacks coming from within their territory. These states frustrate transnational law enforcement efforts by shielding those responsible for cyber attacks from investigation, extradition, and prosecution. In combating cybercrime, the hardest problem is obtaining custody of criminals, without whom there can be no punishment or deterrence of future crimes. A preliminary, albeit limited, step to addressing cybercrime is the Council of Europe's Convention on Cybercrime ("Cybercrime Convention"). The treaty requires state parties to criminalize certain cyber activity such as illegal access, interception and computer forgery and fraud.[371] The treaty also mandates that parties enter into extradition and mutual assistance agreements.[372] As of June 2010, the treaty had only forty-six signatories and only thirty states had ratified it.[373] Some experts agree that the treaty is unlikely to achieve worldwide acceptance.[374] Importantly, two states of major concern with respect to cybercrime, Russia and China, have refused to sign the treaty.[375] Among the signatories to the treaty, preserving sovereignty was a priority that led to the exclusion of any authorization for unilateral cross-border searches, even in the cases of emergency or hot pursuit.[376]

Even with the Cybercrime Convention's concerted effort to combat cybercrime, the particular challenges of investigating crime in the cyber

---

369 *See supra* Part II.B.1.

370 *See supra* Part I.B.

371 Abraham D. Sofaer, David Clark & Whitfield Diffie, *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 185 (2010).

372 *Id.*

373 *Id.*

374 ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 17 (2010).

375 Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 371, at 220.

376 *See id.* at 220, 221.

domain raises doubts as to the long-term effectiveness of a law enforcement approach to the cyber threats. As many cyber experts involved in international criminal cyber investigations have described, "[I]t is very difficult to solve cyber crimes due to cross-jurisdictional difficulties; lack of trained police, prosecutors and judges; [and] problems with digital forensics and evidence . . . ."[377] In pointing out the limitations of the Cybercrime Convention, some have suggested that an international agreement on responsive defensive measures by victim states would be more effective.[378] In circumstances where states may be complicit in criminal activity with little incentive to cooperate in any criminal investigation, the likelihood of detecting and stopping the perpetrators will be low. Such limitations constrain states in countering harmful cyber attacks carried out by state and non-state adversaries.

The international rules governing the use of force also constrain victim states' efforts to counter cyber attacks when those responsible for the attacks are located in the territory of uncooperative states. In April 2007 Russian hackers carried out cyber operations against Estonia, crippling the Estonian government and commercial computer networks. The Estonian Defense Minister claimed the distributed denial of service attacks were equivalent to a conventional military force closing down Estonia's ports.[379] He described the incident as "the first time that a botnet threatened the national security of an entire nation."[380] Some argued that these cyber operations against Estonia triggered the North Atlantic Treaty's ("NATO") Article 5, which declares that an attack against one member is an attack against all members.[381] NATO, however, provided only limited recovery support after the DDOS attacks, leaving open the debate over whether Article 5 can be triggered by cyber attacks.[382]

According to Estonia officials, Russia rejected numerous Estonian requests to help track down those responsible for the attacks, investigate the incident, or

---

377 Rattray & Healey, *supra* note 154, at 75.

378 *Cf., e.g.*, Sofaer, Clark & Diffie, *supra* note 371.

379 Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, J. STRATEGIC SEC., Summer 2011, at 49, 54.

380 Joshua Davis, *Hackers Take down the Most Wired Country in Europe*, WIRED (August 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

381 *See, e.g.*, *id.*; *see also* North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

382 Herzog, *supra* note 379, at 54 (noting that NATO's Computer Emergency Response Team helped restore "normal network operations"); *see also* Davis, *supra* note 380.

stop the attacks against Estonia.[383] To date, attribution directly to the Russian government has not been possible. While no direct links to the Russian government were uncovered, the attacks were linked to nationalist groups "following instructions provided on Russian-language Internet forums and websites."[384] At least one group involved in the attacks had links to the Russian government.[385] Such connections, however, would likely not reach the level of "control" (by the government over the actions of the non-state actors responsible for the attacks) necessary to hold Russia responsible under international law. Yet requiring a victim state to show with "clear and convincing evidence" the direct ties between the government and the hackers, which may be impossible in the cyber domain, would significantly restrict a state's right to respond in self-defense.

In August 2008, Russian military forces invaded Georgia.[386] Prior to the military invasion, the Russians carried out DDOS attacks on Georgian computer systems, which "rerouted [Internet traffic] through Russian-controlled servers and blocked" Georgian government, media, and commercial sites.[387] As with the cyber attacks against Estonia, attribution to the Russian government has not been possible, although some circumstantial evidence suggests that the Russian government was involved in directing, sponsoring, and paying Russian youth groups to carry out the cyber operations against Georgia.[388] According to reports, the attackers who were affiliated with Russian organized crime were "tipped off about the timing of the Russian military operations while these operations were being carried out."[389] In this way, the Russian government can maintain plausible deniability for the cyber attacks, distancing the state from the hackers while passively supporting their actions. Among cyber experts, it is widely thought that Russian government

---

383 ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 27–28 (2010), *available at* http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. For a detailed discussion of the Estonia case, see *id*.

384 *Id.* at 33.

385 Charles Clover, *Kremlin-backed Group Behind Estonia Cyber Blitz*, FIN. TIMES (Mar. 11, 2009), http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

386 Daniel J. Ryan et al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1165, (2011).

387 *Id.*

388 GREYLOGIC, PROJECT GREY GOOSE PHASE II REPORT: THE EVOLVING STATE OF CYBER WARFARE 20–21 (2009), *available at* http://www.fserror.com/pdf/GreyGoose2.pdf.

389 U.S. CYBER CONSEQUENCES UNIT, OVERVIEW BY THE US-CCU OF THE CYBER CAMPAIGN AGAINST GEORGIA IN AUGUST OF 2008 3 (2009), *available at* http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

security services were behind both the Estonia and Georgia cyber operations.[390]

These events illustrate the obstacles involved in transnational law enforcement efforts to combat cyber attacks and the current international legal constraints upon states to act in self-defense when adversary states purposely cause or have others cause harm to their territory. A state's unwillingness to suppress cyber attacks originating within its territory has been used as a shield to deny responsibility for state action, thereby limiting the victim state's right of self-defense. The difficulties of attribution in cyber operations challenge some of the basic assumptions of international law related to use of force in self-defense and state responsibility.

In 2010, the Stuxnet malware infected computers used in the Iranian nuclear program. Cyber security experts have concluded that, based upon the complexity of the computer code, a state most likely developed the malware.[391] To date, there has been no clear evidence linking a particular state to the cyber operation, although some have suggested that the United States and Israel were behind the operation.[392] The effect of the malware was to cause centrifuges to malfunction and ultimately slow down the Iranian government's unlawful nuclear program.[393]

Stuxnet is the first reported incident of a successful cyber operation against state control systems that support the functioning of critical infrastructure.[394] According to former and current U.S. government officials, however, there likely have been many attempts against the United States' critical infrastructure already. Richard Clarke, former national security White House advisor under the Clinton and Bush administrations, warned of the Chinese embedding a "logic bomb" on the U.S. power grid.[395] If the Chinese had

---

390 Herzog, *supra* note 379, at 1180 & n.92.

391 Fildes, *supra* note 252.

392 *See generally* DAVID SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 200–08 (2012).

393 *Id.* at 206.

394 Fildes, *supra* note 252.

395 CLARKE & KNAKE, *supra* note 41, at 54 ("Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability and also thought that it might itself be targeted by cyber war; it has . . . laced U.S. infrastructure with logic bombs."); *see also* Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., April 8, 2009, at A1; Andy Greenberg, *Spies in the Grid: The Feds' Timely Cyber Alarm*, FORBES (April 8, 2009), http://www.forbes.com/2009/04/08/hackers-utilities-cybersecurity-technology-security-power-grid.html.

activated this computer malware, the ramifications of taking down portions of the U.S. power grid would have been potentially catastrophic.

The cases of cyber attacks against Estonia and Georgia demonstrate that an effective strategy to combat cyber attacks by non-state actors requires a mechanism for preventing states from supporting or turning a blind eye to cyber attacks emanating from within. The case of Stuxnet illustrates the capability of cyber tools to comprise critical aspects of a state's national security. As these recent events have revealed, the utility of law enforcement measures and criminal law is seriously limited when states refuse to cooperate in investigations and attribution is a significant challenge for victim states to prove. As mentioned previously, under international law, states can be held accountable for the acts of private individuals who carry out attacks from their territory and cause harm in another state. Under circumstances where law enforcement measures are deemed ineffective in holding a state accountable for stopping the threat, what are the options under international law for the victim state to defend its territory against such threats?

Historically, the international principle of state responsibility has been based on a finding that if the state had direct control over the offending non-state actor, and attribution to the state was feasible, others could hold the state culpable for the offending non-state actor's actions.[396] The international court decisions that utilized this standard of "effective control" in holding the state responsible, however, did not envision the possibility or impact of modern terrorism or the use of the Internet to cause grave harm to states. Certainly, finding a clear case of effective control by a state over a non-state group will likely be impossible in cyberspace, where communications can be made instantly, funds can be shifted relatively anonymously, and actions can be routed globally.[397] Additionally, "notions of 'location' and 'distance' are only loosely correlated between real space and cyberspace . . . [and] files themselves may be distributed across cyberspace, and the number of steps changes with both the specific hyperlinks and with time as loading of the Internet packet switches changes."[398]

---

396 *See supra* note 149–151 and accompanying text.

397 Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyberattacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 981–84 (2011) (cataloguing several shortcomings in the science of tracking cybercrime).

398 Ryan et al., *supra* note 386, at 1169.

In the cyber domain, while states can trace an attack back to a server in another state, identifying who is at the other end of the electronic connection directing the attack can be very difficult and time consuming.[399] With the passage of time, those responsible can destroy evidence eliminating any possible paper trail for investigative purposes. Even when a cyber attack can be attributed to a non-state actor, a victim state seeking not to violate the sovereignty principle is dependent on the assistance of the host state to investigate the attack.[400] Unfortunately, a lack of state cooperation has limited a state's ability to respond to an attack and comply with international law. [401] The primary means through which states have attempted to resolve the dilemma is through criminal laws.[402] The most uncooperative states, however, have been unwilling to enact domestic criminal laws outlawing cyber attacks or have failed to prosecute those who have violated the laws.[403]

States that fail to take the initiative to prevent cybercrime and cyber attacks can be held responsible for any breach to international peace and security caused by resulting cyber operations.[404] It may not be realistic, however, to expect states to be able to completely prevent cyber attacks by non-state actors within their territory from ever occurring. Therefore, the dispositive factor in implementing the norm of state responsibility and evaluating whether the state has fulfilled its duty to prevent non-state actors from conducting cyber attacks from its territory will be in changing the conduct of the host-state itself when addressing potential threats. As the norm of state responsibility has evolved since 9/11, a state may be found to have breached its duties not only through affirmative efforts, but also through what it failed to do to prevent the threat from materializing.[405] Passiveness or indifference by the host state to the activities of cyber hackers could thus result in the state being held responsible for the effects of the cyber attack even though the state did not sanction the attacks.

Creating a legal regime based upon the norm of state responsibility in cyberspace will be a challenge given the limited capabilities for attribution, the

---

399 Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 232–35 (2002).

400 *See* Vatis, *supra* note 375, at 220, 221.

401 WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE vii (2003).

402 Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, MIL. L. REV., Fall 2009, at 1, 6.

403 *Id.* at 45–46.

404 Proulx, *supra* note 173, at 660.

405 *Id.* at 629.

lack of ability to have significant oversight, and the material power of those who are actively harboring and supporting hacker activity. However, establishing a standard for the norm of state responsibility in the context of cyber attacks with implied liability to the state based upon the actions of the state offers hope for a normative framework with which to diplomatically engage those states harboring hackers.

Given that the U.N. Security Council could have authorized the use of force against al Qaeda under Article 42 of the U.N. Charter, it is significant that instead it did so under Article 51.[406] This is of critical importance in the development of cyberspace responses. As individuals and non-state actors are more than capable of inflicting damage and undertaking cyber attacks, this has laid the groundwork for state retaliation against such attacks. Giving even greater support for the action against a non-state actor was the widespread international support for the U.S. military action in Afghanistan from organizations such as NATO and the Organization of American States, as well as numerous states such as Russia, China, India, Japan, South Korea, Pakistan, Saudi Arabia, and Egypt.[407] The international response to 9/11 seems to have eliminated the evidentiary problems involved in identifying the original act as wrongful and directly sponsored by the state, thereby justifying a military response to the attacks.[408] From this new line of reasoning, once an attack is carried out to the detriment of the victim state, the international community will look at the issue more broadly as an attack emanating from another territory and focus on how the host state could have limited or avoided its responsibility for that attack.

For counterterrorism policy, this standard offers a legal framework that is more practically viable than one based on a direct causal relationship between the non-state actor, al Qaeda, and the government, the Taliban.[409] Based on this standard, if the Taliban could not demonstrate that it conducted its due diligence in trying to prevent al Qaeda from launching attacks from Afghanistan, then the Taliban would be in violation of its international obligations and thus be responsible for the 9/11 attacks. As with counterterrorism policy, this new framework for the norm of state responsibility for cyber attacks will be based on an ex post facto factual evaluation of the host state's actions prior to the attack, to be performed on a

406 U.N. Charter art. 51.
407 Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).
408 Proulx, *supra* note 173, at 647.
409 Sklerov, *supra* note 362, at 46.

case-by-case basis. In assessing this new framework for the norm, there are steps a state can take prior to any attack emanating from its territory that, while not guaranteeing the prevention of all cyber attacks from occurring, may still lower its legal responsibility for the attack if an attack were to occur from within the state's territory. Importantly, following these steps could lead to a more tempered response from the victim state.

As more and more control systems become automated and people all over the world become reliant on cyber systems, the scope, veracity, and volume of malicious hacker activities are all likely to increase. There needs to be at least a basic norms-based framework in place for responding to these activities in order for a responsible diplomatic or military response to be formulated. In light of the challenges that cyberspace offers to the security of the international community, strengthening an international norm of state responsibility may provide the precise framework necessary for diplomatic negotiations and a more secure and accountable cyberspace environment. Given the decisions of the ICJ, as discussed above, and the court's trend in its application of Charter norms concerning *jus ad bellum* (limiting a victim state's right to respond in self-defense), it may be up to states to take a more active role. Recognizing that international law is not solely made by courts, but also by states, and given the importance of a legal structure to ensure order in the cyber domain and minimal aggression, states should respond by individually and collectively establishing the principles of state responsibility that will ensure that cyberspace does not become space for "secret wars" where states must forfeit their rights of self-defense or else be accused of violating international law. The standard offered in Part IV of this Article may assist the move in this direction through cooperative efforts.

The central thrust of the diplomatic discussions on a norm of state responsibility relevant for cyber security would focus on the following host state's actions: codifying domestic criminal legislation against hacking, utilizing these laws to prosecute those that break the law, cooperation with other nations in sharing information, and allowing others to investigate within the host state's territory.[410] Assessing state responsibility would examine whether these state actions were in line with the state's legal obligations to prevent a cyber attack's occurrence. Under this standard, while a host state may not be responsible for the acts of private individuals who have taken down a server in the United States, it will be responsible if it fails to take all

[410] Sklerov, *supra* note at 402, at 62.

necessary steps to protect the security and misuse of the Internet in its country or to minimize and mitigate the damage caused by any misuse.

As Howard Schmidt, the former White House cyber security coordinator, described in 2010, "One of the key things has been going back to the countries that it appears it's coming from and saying: 'If it's not you, you need to investigate this.'"[411] A state's failure to take steps to investigate and stop the perpetrators can be followed by a measured response in self-defense.[412] International law allows for proportionate countermeasures in response to harm originating from a state,[413] even if the government is not behind the harm.[414] Before a countermeasure is taken, however, the victim state may be required to make a determination about the target state's reason for its failure to investigate, calling upon the target state to cease in the wrongful actions and offering assistance.[415]

According to Article 49 (1) of the Articles of State Responsibility, the sole permissible purpose of countermeasures is to induce the responsible state to resume compliance with its international legal obligations. If the target state resumes its international legal obligations then the victim state can no longer continue countermeasures. In the case of cyber operations, for example, if the state lacks the resources to investigate cyber attacks from its territory, the victim state may be required to offer assistance to the target state before any forcible countermeasure would be justified. If the target state accepts the assistance the victim state may lose its right to invoke countermeasures since the target state appears to have resumed its international obligation to try to prevent harm to others from its territory. If, however, the offer of assistance was rejected by the other state, the victim state may respond with proportionate

411 Joseph Menn, *US Cybercrime Chief Wary on Provoking China and Russia*, FIN. TIMES, March 5, 2010, at 4.

412 Sklerov, *supra* note 402, at 13.

413 Countermeasures are actions that are taken in response to a violation of international law by another state and that would be unlawful by themselves were it not for that previous action of the other state. *See* Responsibility of Germany for Damage Caused in the Portuguese Colonies in the South of Africa (Port. v. Ger.), 2 R.I.A.A. 1011, 1028 (1928) (requiring that the countermeasures be proportionate to the gravity of the initiating breach); *see also* Rep. of the Int'l Law Comm'n, 52d Sess., U.N. GAOR, 55th Sess., Supp. No. 10, at 124, U.N. Doc. A/55/10 (2000) ("Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."); Gabcikovo-Nagymoros Project (Hung. v. Slovk.), 1997 I.C.J. 7, para. 85 (Sept. 25) (applying the International Law Commission Draft Articles).

414 *See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE, 11, 17–18 (2011).

415 TALLINN MANUAL, *supra* note 18 (manuscript r. 9, para. 8).

force.[416] Developing the requirement to offer assistance may help avoid forcible escalation in the case of cyber attacks. Furthermore, the availability of countermeasures in the context of cyber operations increases the available options of the victim state for a proportionate response that would be lawful.[417]

IV. LOOKING AHEAD

The development of large-scale arms control treaties on cyber conflict does not seem probable, at least not for several decades. In the late 1990s, Russia first proposed a treaty banning espionage and the use of malicious code in cyber conflict.[418] The United States, however, argued then that any new treaty in cyberspace would limit the United States' ability to defend itself in a cyber conflict. Although today the United States is reconsidering its position,[419] there are still some major hurdles to agreement on any new cyber treaty.[420] Verifying compliance would be difficult if not impossible. Because attribution is so challenging in cyber operations, state signatories would be able to violate the terms of the treaty with little likelihood that the United States would be able to prove the violations.[421] Yet the United States and others have recognized that a determined adversary acting in cyber could cause great damage to a state's critical infrastructure.[422] Concerns about the cyber threat are not limited to the actions from state adversaries. Cyber attacks from non-state actors, whether criminal syndicates, terrorists, or political hacktivists, are widely viewed as a core threat to world order and the security of the Internet. In practice, it seems likely that a nation severally harmed by a cyber attack would find support from other nations for an expanded right to self-defense; third-party states are not likely to deny a victim state military redress in the name of quickly changing international law. Certainly, state practice in this area will determine how the law develops. The norm of state responsibility can provide states with the

---

416 The majority of the Group of Experts concluded that "cyber countermeasures may not involve the threat or use of force . . . ." *Id.* (manuscript r. 9, para. 5). A minority of the Group of Experts accepted the approach of Judge Simma in the ICJ's Oil Platforms case that proportionate countermeasures could involve a limited degree of military force. *Id.* (manuscript r. 9, para. 7). All Experts agreed that cyber countermeasures could not rise to the level of an "armed attack." *Id.* (manuscript r. 9, para. 5).

417 *Id.* (manuscript r. 9, paras. 11–13).

418 A.A . Streltsov, *International Information Security: Description and Legal Aspects*, DISARMAMENT F., 2007 no. 3, at 5, 6, *available at* http://www.unidir.org/pdf/articles/pdf-art2642.pdf.

419 *See* John Markoff & Andrew E. Kramer, *In Reversal, U.S. Talks to Russia on Web Security*, N.Y. TIMES, December 13, 2009, at A1.

420 Jack Goldsmith, *Cybersecurity Treaties: A Speculative View*, FUTURE CHALLENGES IN NAT'L SECURITY & L., 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

421 *Id.*

422 Obama, *supra* note 3.

opportunity to develop agreements on how such disputes are resolved and potentially limit the escalation of cyber conflict between states.

The development of a norm (shared expectation of proper behavior) like state responsibility, however, offers the possibility of broader international participation, as norms are not written, contractual legal obligations. In normative development, the first step is to generate and obtain agreement on the norm particulars between like-minded states. Over time, other more reluctant states and organizations may become "socialized" into deeper acceptance of the norm, creating a spillover effect to other states as engagement on the issues becomes more widespread. As with international norms in other areas, the easier it is for states to comply with the norm, the more likely the norm will "cultivate" and spread.

The United States has recently begun informal discussions with Russia and China, two states that generally do not agree with the United States' position on cyber activities.[423] These discussions can serve as a foundation upon which to build a greater consensus in the future. Although problems may arise from states still being in the early stages of learning and developing shared cyber norms, there is a remarkable similarity to the normative learning curve of the 1950s at the beginning of the nuclear era.[424] Building upon already existing norms about self-defense and the use of force will increase the likelihood of the norm's acceptance. While the United States has begun the process of articulating and promulgating the norm of state responsibility, these steps are not sufficient to ensure changed behavior by states. Nevertheless, if the United States champions the norm, its status as a major stakeholder in cyber security will increase the likelihood of its dissemination and internalization by other states. These are necessary stages in normative development if state behavior is realistically expected to change. Furthermore, if states like the United States offer technical, investigative, or financial assistance to other states that lack the domestic resources to undertake investigations, it will be easier for some states to comply with the norm. This in turn will further the chances for the norm's cultivation. As states like Russia and China engage diplomatically on the topic of state responsibility in the cyber domain, it may be possible to generate enough traction for other states to buy into the norm. Engaged discussion

---

423 Roger Hurwitz, *Depleted Trust in Cyber Commons*, STRATEGIC STUD. Q., Fall 2012, at 20, 20.

424 *Cf.* Joseph Nye, *Power and Security in Cyberspace*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE, *supra* note 154, at 5, 21 (noting the presence of a modern learning curve for the development of international cyber law norms).

between states could help develop common perceptions and more commonly agreed-upon norms.

This Article has supported the notion of the evolution of the norm of state responsibility, as it developed after 9/11, in the context of cyber attacks. Aside from enhancing the legitimacy of international efforts to combat cyber attacks, this model would also foster states' comparative policy-making and collaborative efforts. Under international law, multilateral collaboration should be preferred over unilateral state action in instilling a preventive character to forcible self-defense actions. In this spirit, states could engage in significant risk control and risk assessment of possible cyber attacks and, hopefully, encourage multilateral, or at minimum, initially bilateral exchanges of information and intelligence, along with financial "red-flagging" of cyber assets. In addition to sending a message of deterrence to complacent governments, this approach would also provide states with a forum to voice and test out their cyber security policies. As the *2011 International Cyber Space Strategy* noted, "Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation are needed to confront those actors who would seek to disrupt or exploit our networks."[425]

A. A Standard for Determining When to Use Force Against a Non-State Actor

1. The "Unwilling and Unable" Test Applied in International Armed Conflict Between Belligerents[426]

The roots for the "unwilling or unable" test come from the neutrality laws that are applicable during international armed conflict.[427] These laws are articulated in the Hague Conventions V and XIII and in customary international law.[428] The purpose of the neutrality laws is to ensure that those states not participating in an armed conflict (neutrals) do not sustain injuries as a result of the conflict and their rights are protected. They also guarantee to those states in the conflict that the neutral states will not assist any of those parties in the conflict. For example, the neutrals are not to permit their territory

---

425 2011 INTERNATIONAL CYBERSPACE STRATEGY, *supra* note 15, at 21.

426 *See* Deeks, *supra* note 276, at 483–550 (offering an analysis of the unwilling and unable test, explaining how it arises in international law as part of a state's inquiry into whether it is necessary to use force in self-defense).

427 MORRIS GREENSPAN, THE MODERN LAW OF LAND WARFARE 379–80 (1959).

428 *See* Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 205 CTS 299, Oct. 18, 1907; Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, 205 CTS 395, Oct 18, 1907.

to be used by a party to the conflict as a safe harbor or a place from which to launch attacks.[429] These laws seek to balance the right to engage in lawful operations with the right of neutral states to remain protected from the conflict. This is similar to the *jus ad bellum* principle seeking to balance a victim state's right of self-defense with the right of territorial sovereignty of other states.

Some have argued that the neutrality laws are no longer relevant in the post-Charter era.[430] Even if the neutrality laws are "dead," the purpose and intent of the laws are still relevant when non-state actors may be using the territory of a state (maybe innocent of committing any wrong doing or maybe supporting or sponsoring the illegal activity of the non-state actor) to conduct attacks. The prior existence of the "unwilling or unable" at least grounds the current use of the test in historical legal context. Importantly, because states use the language of the test today to justify uses of force against non-state actors, it is important to investigate the content of the test.

Under these laws, neutral states must not permit belligerents to violate their territory and must take steps to quash such violations.[431] If a belligerent group violates the territory of the neutral state, the neutral state is expected to use "due diligence" in its efforts to prevent violations of its neutrality.[432] So assuming a state is not responsible for the attacks (i.e., it is neutral), then, in line with the purposes of these laws, that state must take steps to prevent the non-state actor from using its territory to commit attacks. If the neutral state uses the means at its disposal, it cannot be accused of violating international legal obligations and cannot incur state responsibility, even if it fails to repel the offending group.[433]

However, what if the neutral state cannot fulfill its obligations in preventing a party to the conflict from using its territory to carry out attacks against another party to the conflict? The military manuals of states and opinions of commentators have recognized that states would not and could not tolerate being left with no recourse if the neutral state was not successful in repelling other belligerents from violating the neutral territory, thereby effectively launching attacks against the victim state.[434] For instance, the military manuals of the United States, the United Kingdom, and Canada

429 DINSTEIN, *supra* note 182, at 25.
430 GREENSPAN, *supra* note 427, at 536.
431 *Id.*
432 STEPHEN NEFF, THE RIGHTS AND DUTIES OF NEUTRALS: A GENERAL HISTORY 211 (4th ed. 2000).
433 *See* DINSTEIN, *supra* note 182, at 216.
434 GREENSPAN, *supra* note 427, at 536.

specifically refer to the "unwilling or unable" test in assessing the right to recourse within the territory of a neutral state, establishing the norm as well-embedded within state practice.[435] The practice by states revealed that their interpretation of the neutrality laws meant that the victim state was permitted to use force on a neutral state's territory if the neutral state was unable or unwilling to prevent violations of its neutrality by one party waging war against another state.

The test of "unwilling or unable" was used by parties to a conflict to guide them in enforcing the neutrality laws in the face of violations by their enemies or by neutral states. The San Remo Manual on International Law Applicable to Armed Conflict at Sea, drafted in 1995 by international legal experts but not binding law, addresses the unwilling or unable test and puts some restrictions upon the test. The manual states that when a neutral state fails to prevent a belligerent party from violating its neutral territorial waters, the state contemplating force must first give the neutral state notice and a reasonable time to terminate the violation before using force.[436] Furthermore, the violation must constitute a serious and immediate threat, and there must not be any other alternatives besides using force in order to stop the violation.[437]

2. The Test Applied in Use of Force Self-Defense Against Non-State Actors

An early case using the test with respect to non-state actors was the *Caroline* incident. Often cited for providing the basic rules for using force in anticipatory self-defense, it also is an "unwilling and unable" test case. As Abraham Sofaer noted:

> The principal difference between them was the claim by the British that the [United States] was either unable or unwilling to stop the rebels within its territory from attacking Canada. The [United States], on the other hand, insisted that it was adequately fulfilling its obligation to prevent the rebels from attacking Canada from [U.S.] territory.[438]

---

435 *See* DEP'T OF THE ARMY, THE LAW OF LAND WARFARE, FIELD MANUAL 27-10, para. 520, July 18, 1956; OFFICE OF THE JUDGE ADVOCATE GEN. (CANADA), LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS, JOINT DOCTRINE MANUAL, para. 1304(3), August 13, 2001; U.K. MINISTRY OF DEF., THE MANUAL OF THE LAW OF ARMED CONFLICT- AMENDED TEXT 01/04, para. 13.9E (2004).

436 SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICT AT SEA, para. 22 (Louise Doswald-Beck ed., 1995).

437 U.K. MINISTRY OF DEF., *supra* note 435, 13.9E.

438 Abraham D. Sofaer, *On the Necessity of Pre-emption*, 14 EUR. J. INT'L L. 209, 216–17 (2003).

Recently, in the context of extrajudicial killings of terrorists, the Special Rapporteur for the U.N. Human Rights Council noted:

> A targeted killing conducted by one State in the territory of a second State does not violate the second State's sovereignty if either (a) the second State consents, or (b) the first, targeting, State has a right under international law to use force in self-defence under Article 51 of the UN Charter, because . . . the second State is unwilling or unable to stop armed attacks against the first State launched from its territory.[439]

This "unwilling or unable" test is suitable to be applied to non-state actors during a time of peace as well as neutral states during a time of armed conflict. Although the sources of the duties under international law are different, the equities of the states at issue are the same and therefore the purpose and intent of the laws are what matters. The purpose of the neutrality laws is to ensure that neutral states during a time of international armed conflict do not allow their territory to be used by a belligerent party to the conflict in order to seek safe harbor to plan and carry out attacks against an enemy.[440] The source of the duty on the neutral state comes from either a neutrality treaty to which it is a signatory or from customary international law. Under the laws related to use of force at a time of peace, the issue is ensuring that states do not allow their territory to be used by non-state actors to initiate and carry out armed attacks against the victim state. A state's duty to prevent non-state actors from carrying out attacks from its territory comes from the international rule codified in the 1970 *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United States*.[441]

The principle of sovereignty requires that both neutral states during times of conflict and states during times of peace desire to preserve their territorial integrity. One might argue, as this Article as done, that this is part of the responsibility of all sovereign states. Both types of states are responsible for fulfilling their international legal obligations. Likewise, when a state has been attacked by non-state actors from another state's territory, it does not matter whether that state is a belligerent in conflict or a victim state during a time of

---

[439] U.N. Human Rights Council, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions* para. 35, U.N. Doc. A/HRC/14/24/Add. 6 (May 28, 2010) (footnotes omitted).

[440] *See generally* Deeks, *supra* note 276, at 497–501 (providing background information on the law of neutrality).

[441] *See* G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028, at 123 (Oct. 24, 1970).

peace; both types of states have an interest in stopping the attacks and avoiding conflict with the neutral state.

3. Developing a Standard

Developing a workable standard for determining when it would be lawful to use force against a non-state actor in self-defense in another state's territory after suffering a cyber attack would be useful considering that courts, scholars, and treaty law have not provided clear details for such a standard upon which state's actions will be judged. To identify what a standard may look like, the rest of this Article will draw upon the case law, commentaries, state practice, and treaty and customary law principles to suggest specific criteria for the standard.

The usefulness of such a standard ought to be clear. In the absence of clear legal guidance, a decision-maker is left wondering what criteria he ought to use when deliberating about the legality of the use of force under the circumstances. Knowing how to employ a test under international law properly is important if the goal is that the actions are considered legal and legitimate. A vague or broadly ambiguous test without content is meaningless. Hopefully, the criteria offered in this Article will be useful to determine what assessments a victim state should make before using force against a non-state actor within the territory of another state in the context of a cyber attack, and also how the victim state should make those assessments.

As international law scholars have noted, international norms are more likely to be viewed as legitimate if there is clarity about where the boundary exists between what is permissible under the norm and what is not. According to Thomas Franck, for example, when there is no ascertainable understanding about what is permitted or prohibited by an international norm, "states are unlikely to defer opportunities for self-gratification. The rule's compliance pull evaporates."[442] Some practical benefits to the victim state in utilizing the criteria offered below are that the victim state would have the opportunity to acquire and assess information on the target state that it otherwise would not have known, it would improve its decisional process with specific action items, and, importantly, it would be able to defend its actions before the Security Council, international courts, or other states, against a clear standard. In effect, criteria allow victim states to "build a case" for a legal self-defense response.

---

[442] Thomas M. Franck, *The Power of Legitimacy and the Legitimacy of Power*, 100 AM. J. INT'L L. 88, 93 (2006).

Certainly, however, one does not want a test so undefined that it would allow victim states to abuse it by using the broad terms of "unable or unwilling" to justify the use of force when the target state in fact was able and willing to act to stop the attacks. Nor does one want such broad language of an undefined test to be used as a whip against a victim state that has been attacked and used force in self-defense in good faith, trying to follow the test, and then is punished by an international court or public outcry. Or, it may be that a victim state with a legitimate right to use force under the test refrains from doing so and leaves itself undefended against real threats because of uncertainty of the meaning of the test or expectations by international bodies about the test. In practice, this last scenario is unlikely to happen when the victim state's national security is at risk because a victim state will likely ignore a test that fails to provide for a legitimate right of self-defense when national security is at stake. The danger in this case is that if a state ignores the test, there will be even more uncertainty about the law and its applicability could possibly lead to more uses of force than necessary.

As this Article stated at the beginning, the goal here is to provide a test that would produce an appropriate balance between the right of sovereignty and a victim state's right of self-defense. As mentioned previously, there exists a tension between the two, particularly in the area of use of force. However, these factors for a better understanding of the test may help find the appropriate balance between these two principles of international law.

The U.N. report, *A More Secure World*, recommended that the U.N. Security Council adopt guidelines to govern when it would authorize the use of force, and thereby increase the legitimacy of those authorizations.[443] As state practice and U.N. Security Council inaction in the area of use of force continues, it will likely be states more often than the U.N. Security Council that will be making decisions (unilaterally or collectively) about whether to use force. While the report's recommendation was important for the Security Council, such a test is arguably more readily needed by states. Unfortunately, based upon the international court cases discussed previously in this Article, the courts do not appear likely to deliver a clearly defined test for states to follow. Most likely it will be up to states, through practice, to develop the law in this area and, hopefully, they can produce a clearer test by doing so. States may do a service to the U.N. Security Council and international courts by using such a test, for in assessing the legality of the actions of a state after the fact,

---

[443] U.N. Report, *A More Secure World*, *supra* note 1, at 57.

the U.N. Security Council and the courts will have a useful tool by which to judge the actions of the state using force. Such a tool would be very useful in further developing the law in this area.

B. Criteria for the Victim State and the Target State

First, to set forth a basic assumption as part of the foundation for the criteria, it will likely be impractical to dictate a specific agreed-upon burden of proof with respect to the level of certainty about the threat a victim state must face before using force in another state. However, a minimum threshold of good faith by the victim state is warranted. In following a standard, especially if that standard has specific content, a victim state could use the standard to support an argument of its good faith efforts.

The following criteria are offered to a victim state deliberating whether to use force in self-defense against a non-state actor in another state's territory. These criteria are also offered to the target state assessing the legality of a use of force in its territory by the victim state. As cyber conflict becomes more of a reality, these criteria may prove useful as states assess whether to use force in response to cyber attacks.

1. Prior Notification to the Security Council

A victim state should report a serious use of force within its territory by a non-state actor to the U.N. Security Council whether or not it has decided to use force in self-defense. This provides that victim state with the opportunity to articulate its assessment of the threat level it perceives, offering the Security Council all relevant information that it may be able to provide. This can also serve to put the target state on notice that it may be considering the use of force in self-defense. When providing information on the threat, the victim state should describe the following relevant details: (1) the geographic scope and intensity of the non-state actor's past and current activities against the victim state and any other states the actors have targeted; (2) the sophistication of the attacks and any information that indicates potential future attacks from the actor; (3) the characteristics and number of actors operating within the target state as well as the level of seniority of those actors operating in that area; (4) the imminence of any future attacks; and (5) any links between the non-state actor and the target state.

2. Prior Notice to the Target State: Seek Consent or Cooperation from the Target State

A victim state should report serious use of force within its territory by a non-state actor to the target state. Putting the target state directly on notice avoids any controversy over whether the state had "actual" versus "constructive" knowledge of the ongoing threats from within its territory. Although there is a debate as to whether actual knowledge of the threat is required before the victim state responds to the threat, this step would clearly resolve any disagreement about knowledge by the target state. This is also the opportunity for the victim state to provide a direct threat assessment to the target. Especially if the victim state did not notify the U.N. Security Council and provide a threat assessment then, or if the threat assessment was not made public at the time, the victim state should provide this information to the target state.

If the victim state obtains the consent of the target state to use force within its territory, the victim state would not need to go through any further inquiry with respect to the criteria offered here. Under international law, as previously discussed, consent by the target state is an exception to the prohibition to use force against another state.[444] Furthermore, if the target state denies its consent, the denial can be relevant in assessing the other factors of the criteria below. The request for consent alone, even if denied, may minimize international complaints if the victim state ultimately uses force unilaterally.

3. Request that the Target State Address the Threat and Provide a Reasonable Amount of Time in Which to Do It

By providing a threat assessment to the target state, the victim state has assisted the target state in seeking to address the threat. The victim state can request that the target state arrest individuals, eject them from the territory, turn them over to the victim state, or use forcible measures to stop the threat. In making the request, the victim state could provide specific information, including intelligence information, that would assist the target state in fulfilling its obligation to address the threat. For example, the victim state may have intelligence information about the specific location of the non-state actors.

---

444 Michael Byers, *Letting the Exception Prove the Rule*, 17 ETHICS & LEGAL AFF., March 2003, at 9, 14 (noting the "undisputed fact that a state can freely consent to having foreign armed forces on its territory").

However, this step would not necessarily be required as the victim state assessed the facts. For instance, if the victim state had credible information that the target state would warn the non-state actor and not take steps to stop the threat, the victim state would not be required to provide this notice and a request to the target state. The victim state could take a number of factors into consideration before deciding whether to provide the information to the target state requesting that it take action. The victim state could, in this situation, consider whether the target state had previously made public statements in support of the non-state actors or provided actual support to them even after an prior incident. It could also consider whether that state, because of domestic pressure, would not likely take any action against the actors. For example, if the domestic political pressures were obviously such that the state would not be able to use its resources against the actors without great political cost or upheaval, the victim state might decide not to request help from the target state. The victim state, however, would likely receive international condemnation if it failed to make such a request.

The burden here is on the target state to do something or provide relevant responsive information to the victim state. The burden is shifted to the target state to show certain facts since it has the greatest access to the facts. As the ICJ has noted:

> [T]he fact of this exclusive territorial control exercised by a State within its frontiers has a bearing upon the methods of proof available to establish the knowledge of that State as to such events. By reason of this exclusive control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence.[445]

In making such a request to the target state, the victim state must assess what reasonable amount of time would be appropriate to allow the state to resolve the threat. Much of this decision would rely on the past practices of the target state as well as an assessment of its actual capabilities to do anything. For example, if the target state had limited or ineffective law enforcement, intelligence, or military tools to use, or if it lacked the political will or domestic criminal laws, then the victim state would likely not have to allow much time to pass before taking action. What constitutes a reasonable amount of time would also depend on the imminence and gravity of the threat. If the

---

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

threat was serious and imminent, with "no moment for deliberation,"[446] or if another attack was already being planned, the victim state might have no other choice but to act in a proportionate manner to the threat without asking for assistance from the target state.

4. Reasonably Assess the Target State's Control and Capacity Within Its Territory To Prevent or Stop the Threat

If the victim state has reservations about the target state's ability to stop the threats based upon limited law enforcement, intelligence, or military capabilities, the victim state must make a reasonable assessment about the likelihood that the target state could actually have an impact on stopping the threat, even if it wanted to. For example, it might be the case that the area in which the threat is operating is in a location where the state has no power or no ability to control. In the cyber context, if a state does not have legal authority over its Internet Service Providers to stop malware from being launched from its territory, then it will likely not be able to stop the cyber attacks. If it lacks law enforcement tools or does not have any domestic legislation criminalizing hacking, it will be limited in how it stops such cyber threats. A review of a target's domestic laws and criminal investigative authorities would be relevant for a determination of its actual control over its territory.

If the victim state publicly provides information describing the lack of control that a target state has over the private entities or corporations that may be responsible for the cyber attacks, for example, the victim state may lessen the international criticism for its use of force. If the target state has failed to pass any effective cyber security measures that attempt to prevent harmful malware from transiting or being launched from its territory, the victim state will likely have a stronger case that the state is unable to stop or prevent threats. In this regard it is important that the United States continues to work with the private sector in sharing cyber threat information and seeking to take domestic action to minimize harmful cyber operations emanating from the United States and harming others in another state territory."

Reviewing the target state's capacity and control within its territory in this manner will reflect positively on the victim state as it is conducting due diligence in assessing the need to use force to stop the threat. Ultimately, the target state will need to show that it has taken due care in its efforts to prevent

---

446 Caroline Letters, *supra* note 356, at 198.

and stop attacks against the victim state.[447] Although preventing all cyber malware from being launched from a state's territory may be impossible, the test would not require that all such incidents be prevented; rather, the target state would need to show it has taken concrete steps to minimize or eliminate the threats. It may be that the more serious the threat, the less likely the victim state will be able to deal with it if it lacks the means. Under these circumstances, the target state should be willing to accept the victim state's help in stopping the attacks.

5. Reasonably Assess the Target State's Proposed Means To Stop the Threat

Although it may be unlikely that a target state provides a proposal for stopping the threat, in the case that it does, the victim state must reasonably assess whether the offered proposal will be effective and sufficient.[448] In reviewing any such proposal, the victim state would have the opportunity to gauge whether the state is able and willing to stop the threat. Based on the information presented, the test would be what a "reasonable state" believes would achieve the goal of stopping the threat.[449] Whatever one may believe a "reasonable state" is, in this context, a reasonable state would review the proposal in good faith considering what it believes to be necessary steps to stop the threat and the limitations that any state would likely have, given the circumstances.

As has been recognized with terrorism, it is even more unlikely with cyber attacks that a target state will fully be able to stop all threats originating from its territory. In the case of cyber attacks, most of the infrastructure that cyber attacks will traverse is owned and operated by the private entities and not the government. Although the victim state must decide the proposed plan is sufficient to meet the threat, once a victim state accepts a proposal from the target state, it is obligated to review the plan in good faith. If a victim state fails to do this, it likely that its use of force would not be seen as legitimate.

---

[447] The Group of Experts that drafted the Tallinn Manual was unable to reach consensus on whether a State would be in violation of its obligation to prevent harm to another State from its territory if the State failed to "use due care in supervising cyber activities on its territory" and was unaware of the actions in question (the State should have known) versus the State being in violation of the obligation when it actually knows of the attack. TALLINN MANUAL, *supra* note 18 (manuscript r. 5, para. 11).

[448] *See id.* (manuscript r. 5, para. 4).

[449] *See* Schmitt, *supra* note 14, at 40 (noting that "reasonable states do not act precipitously, nor do they remain idle as indications that an attack is forthcoming become deafening").

6. Reasonably Evaluate Prior Interactions with the Target State and the Target State's Prior Interactions with the Non-State Actors

In order to assess the target state's willingness to respond to the threat, the victim state should review the target state's responses to any prior requests to stop the threats from this particular non-state actor or other similar non-state actors that had been operating from within the target state. It would be important that any past incidents of non-state actors conducting harmful operations from the target state's territory be reported to the U.N. Security Council and the target state, to ensure that a historical record is made. This way, any victim states could refer to the past incidences to draw inferences about the likelihood of the target state responding to the request to stop the threat. Even if non-state actors are not the same, but ones conducting the same type of harmful actions against other states (i.e., botnet attacks), a victim state can draw inferences from past cases in assessing the current chances of the target state taking action against a threat.

Prior warnings provided to the target state, regardless of whether any victim state used force in the prior cases, serve to show a trend in the target state's behavior and are relevant in assessing whether the state is truly willing to respond to the threat. Particularly if the prior requests have gone unanswered by the target state, the victim state can draw some strong inferences against the state's willingness to take the threats seriously.

If a target state has never before had a serious cyber attack launched from its territory by a non-state actor, the victim state should be hesitant to conclude, without further information, that the target state is unwilling or unable to address the threat. In the case in which a victim state is contemplating the use of anticipatory self-defense against the territory of another state, the victim state must be especially careful because there may be no historical evidence of attacks launched from the target state. The accuracy of the victim state's information related to the seriousness and location of the threat within the target state will be especially important under these circumstances.

7. Evaluating the Victim State's Responsive Measure To Use Force: Proper Purpose, Last Resort, Proportionality, and Balance of Consequences.

In determining whether to use force in self-defense, the victim state should also evaluate the remedial measures that it is considering. First, the victim state must make an honest assessment of the nature, scale, and scope of the harm

that its use of force will cause. It must be clear that the primary purpose of the use of force is to stop the threat in question. Second, in using force in self-defense, the victim state must always make a determination that its recourse to force in the specific case was the necessary measure at the time, given the circumstances, in order to stop the attacks or prevent further ones from materializing. If the state reasonably believes that there are other alternatives aside from using force, then the state must pursue those options before using force. Third, the victim state must determine that the force used is of the scale, duration, and intensity that is minimally necessary to meet the threat. And fourth, an assessment must be made as to the reasonable chance of the use of force being successful in meeting the threat in question with the consequences of action not likely to be worse than the consequences of inaction, to include potential injuries to innocent third parties.