9. Developing norms for cyber conflict

*William C Banks**

1. INTRODUCTION

The prospect of cyber war has evolved from science fiction and doomsday depictions on television, in films and novels to reality and front page news. As early as 1982, a little-noticed but massive explosion of the trans-Siberian pipeline was caused by malware apparently inserted into Canadian software by the CIA. The CIA and Canadians knew that the software would be illegally acquired by Soviet agents. Although the incident greatly embarrassed the KGB, the Soviets never disclosed the incident or accused the United States of causing it. If a US missile had struck the pipeline, the Soviets would have expressed their outrage publicly and almost surely would have retaliated.[1]

As the Internet grew exponentially over the next quarter century, so did the frequency and variety of cyber intrusions. By 2012, reports confirmed that the Stuxnet malware attack on the computers that ran Iran's nuclear enrichment program was carried out as part of a larger Olympic Games campaign of cyber war against Iran begun in 2006 by the United States and perhaps Israel. This use of cyber-weapons to attack a state's infrastructure became the second (following the Siberia explosion in 1982) known use of computer code to affect physical destruction of equipment—in this case Iranian centrifuges—instead of disabling computers or stealing data.[2] Like the Soviet Union in 1982, Iran did not acknowledge the cyber-attack. However, in 2012 Iran released the Shamoon virus in a major cyber-attack on US ally Saudi Arabia's state-owned oil company, Aramco. Shamoon replicated itself inside

* The author is grateful to Kyle Lundin for excellent research assistance.

[1] Brett Stephens, 'Long before There Was the Stuxnet Computer Worm, There Was the 'Farewell' Spy Dossier', *Asian Wall Street Journal*, 19 January 2010.

[2] See David E Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times* (2012).

30,000 Aramco computers, destroying the computers and disrupting operations for nearly two weeks.[3]

In 2013, the US Director of National Intelligence named cyber as the number one strategic threat to the United States, ahead of terrorism.[4] Increasingly frequent and intense cyber-attacks are mounted at military and intelligence targets, as Edward Snowden demonstrated in 2013.[5] In the United States, our electric grid, municipal water and sewer systems, air traffic and railway control, banking system, and even military operations are persistently subject to cyber penetration. At least as costly and sometimes more destructive, cyber intruders attack businesses and industry. Because industrial control systems in most of the world are connected to the Internet, all of them are vulnerable. In 2009, President Barack Obama said that 'cyberintruders have penetrated our electric grid', and that 'in other countries cyberattacks have plunged entire cities into darkness'.[6]

Nor has it been only nation states that carry out the cyber-attacks. Profit-seeking criminals, ideological hackers, extremists, and terrorists have also directed attacks towards state-owned facilities and infrastructure, and against the private sector. At the same time, there are increasing signs that cyber techniques are now an integral part of heretofore violent conflicts between terrorist groups and states. In October 2015, the US government arrested Kosovar Ardit Ferizi in Malaysia. Ferizi was charged with providing material support to terrorism on the basis of his hacks of a private US company for the purpose of gaining access to personally identifiable information of US military and federal employees. Ferizi allegedly released the information on behalf of the terrorist group the Islamic State (IS).[7] Meanwhile, state and non-state cyber threats now often blend and merge, as privateers operate as surrogates for states and provide cover for state-based actors.[8]

---

[3] See Fergus Hanson, '*Norms of cyberwar in peacetime*', Brookings Institution, 17 November 2015.

[4] Office of the Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (2013).

[5] Joel F Brenner, 'Eyes Wide Shut: The Growing Threat of Cyber Attacks on Industrial Control Systems' (2013) 69 Bulletin of Atomic Scientists 15–20, 16.

[6] Barack Obama, 'Remarks by the President on Security Our Nation's Cyber Infrastructure' 29 May 2009.

[7] Ellen Nakashima, 'At least 60 people charged with terrorism-linked crimes this year—a record', *Washington Post*, 25 December 2015.

[8] US Dept of Defense, *The Department of Defense Cyber Strategy* (2015) 9.

Hostile cyber penetration is now a daily occurrence. The perpetrators are too numerous to count, and the targets continue to expand in number and by type. The frequency, breadth and persistence of an ever wider set of cyber exploitations reflects bad actors racing to the bottom of every data repository that might generate profit or impose costs, inflict pain, instill fear, create inconvenience, or disrupt operations. Some states and private actors justify cyber intrusions on the grounds that their adversaries are pursuing cyber operations against them. Others simply attack, for financial or some other gain or to inflict harm, for whatever reasons.

Despite the growing prominence of cyber threats, international law does relatively little to regulate cyber conflict. For the most part, treaty-based and customary international law provide limits on state but not private actions, and only in conflict that has kinetic consequences. Even as experts recognize that terrorists may engage in cyber war, the international community continues to rely on a legal conception that limits terrorism to 'acts of violence committed in time of peace',[9] a categorization that excludes most cyber-attacks. Despite the growing role of the cyber domain in the security sectors of many governments over the last decade, the legal architecture for cyber pays little attention to cyber-attacks that do not produce harmful effects equivalent to kinetic attacks.

A distinguished International Group of Experts was invited by NATO in 2009 to produce a manual on the law governing cyber warfare.[10] The resulting *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*) defines the scope of their project to include only those forms of cyber-attack that meet the UN Charter and IHL conceptions of 'use of force' or 'armed attack'.[11] Beyond limiting their inquiry into state-on-state cyber conflict to these traditional conceptions, the *Tallinn Manual* restates the consensus view that prohibits 'cyber-attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population'.[12] The *Tallinn Manual* experts concluded that cyber-attacks can constitute terrorism, but only where the attack has been conducted through 'acts of violence'.[13] In other words,

[9] Jelena Pejic, 'Armed Conflict and Terrorism: There Is a (Big) Difference', in A-M Salinas De Frias, Katja L H Samuel and N D White (eds), *Counter-Terrorism: International Law and Practice* (Oxford University Press 2012) 203.

[10] *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

[11] Ibid rule 18.

[12] Ibid rule 36.

[13] Ibid rules 30, 36.

the *Tallinn Manual* concludes that international law proscribes only kinetic harm by states and violent terrorism and thus leaves unregulated an entire range of disruptive cyber intrusions.[14] To the great credit of the NATO Cyber Centre of Excellence, the organizers and Group of Experts are finishing *Tallinn Manual II*, which will consider the application of various customary international law doctrines and principles that could apply to govern cyber conflict where the intrusions do not meet the traditional kinetic thresholds.

As reflected in the *Tallinn Manual*, there is international legal clarity in some cyber conflict situations. In instances where a cyber-attack causes physical destruction and/or casualties at a significant level, a cyber-intrusion may constitute a 'use of force' or an 'armed attack' under the UN Charter. In these extreme circumstances, even where the attacker is a state-sponsored non-state actor, customary law permits a forceful response in self-defense, assuming attribution of the attacker.[15] In addition, whether the Charter criteria have been met is most likely a function of the consequences of the cyber event, and is not dependent on the instrument used in the attack.[16] Apart from this relatively small subset of cyber-intrusions, however, the legal regime remains clouded and ambiguous.

Developing a more fully-formed international law of cyber conflict is complicated by a few unique attributes of the cyber domain. Prompt attribution of an attack and even threat identification can be very difficult. As a result, setting the critical normative starting point for invoking international law is elusive—which is the offending state, and what is the line between offense and defense? Preliminary questions include: Is it lawful to anticipate cyber-attacks by implementing countermeasures in advance of the intrusion? How disruptive or destructive a response does the law permit once a source of the incoming intrusions is identified, even plausibly? If victim states cannot reliably attribute incoming attacks, must they delay all but the most passive responses until the threat can be reliably identified? Beyond challenging threshold questions like these, because cyber-attacks will likely originate from multiple sources in many states, using geography as a proxy for a battle space may not be realistic or useful in the cyber context. Even assuming attribution of incoming attacks, which if any geographic borders should define the scope of a victim state's responses?

[14] Ibid rule 30.
[15] Ibid rule 13.
[16] Ibid rules 11–12.

International law scholars and operational lawyers have struggled in recent years to accommodate IHL and the UN Charter system to asymmetric warfare waged by non-state actors, including terrorist groups. The language and structure of IHL—the regulation of 'armed conflict'—and of the Charter—focusing on 'use of force' and 'armed attack'—present considerable analytic challenges and even incongruities in attempting to fit cyber into the conventional framework for armed conflict, even for state-on-state cyber conflict. Because cyber-attacks may be carried out by states or non-state actors and may occur continuously or in stages with no overt hostility and range from low-level harassment to potentially catastrophic harms to a state's infrastructure, the either/or dichotomies of war and peace and armed conflict/no armed conflict are not in most instances well suited to the cyber domain. Over time, the ongoing struggle to fit cyber into the IHL and Charter categories may threaten their normative integrity and their basic commitment to collective security and restraints on unilateral uses of force.

The core component of the framework for regulating the use of force—the UN Charter—is less important in developing future prescriptions for cyber conflict than customary international law, developed over time through state practice. Most cyber-intrusions for the foreseeable future will take place beyond the traditional consensus normative framework for uses of force supplied by international law. For the myriad and multi-faceted cyber-attacks that disrupt but do not destroy, whether state-sponsored or perpetrated by organized private groups or single hacktivists, much work remains to be done to build a normative architecture that will set enforceable limits on cyber intrusions and provide guidelines for responses to disruptive cyber-intrusions. The next two sections of the chapter first review and assess the historical and contemporary normative justifications for cyber conflict, and then outline the components of future cyber conflict norms.

2. EXAMINING HOW AD BELLUM PRINCIPLES MAY APPLY TO CYBER CONFLICT

Cyber-weapons are adaptable and relatively easy to use. One common view is that because the collective law of war does not reach most cyber conflict, states enjoy relatively new non-kinetic options for achieving their conflict objectives, untethered by law. A state's security objective that may have required the use of military force in the past may now be accomplished through the use of cyber techniques. Better still, a state may be able to act in cyberspace without acknowledging responsibility

for what it has done. In order to place the international legal issues in context, consider these scenarios:

Assume that fictional State A launches a massive malware attack at fictional State B. The botnets and sophisticated software unleashed by the malware cause power failures when generators are shut down by the malware. Train derailments and airplane crashes with hundreds of casualties soon follow, as traffic control and communications systems that rely on the Internet are made to issue false signals to pilots and conductors. Dozens of motorists die when traffic lights and signals malfunction at the height of an urban rush hour. State A acknowledges its responsibility for the cyber-attacks, and it says that more are on the way. Clearly there is an international armed conflict (IAC) between states A and B, and pending Security Council action, B is lawfully permitted by Article 51 of the Charter to use self-defense to respond to the 'armed attack' by A. The Charter and IHL norms provide sufficient ad bellum authority for B to respond to these cyber-attacks.

Assume instead that unknown assailants have launched a series of cyber-attacks on the banking system of a state. The malware is sophisticated; large and small customers' accounts are targeted and account balances are reduced by hundreds of millions of dollars. For the time being the attacks cannot be attributed, but non-state terrorists are suspected in light of intelligence reports. No one has been injured or killed. There is no international armed conflict (IAC), either because there is no known state adversary and/or because there has been no 'attack' as contemplated by Article 49 of Additional Protocol I. (Additional Protocol I was added to the 1949 Geneva Conventions in 1977, and Article 49 expands on the definition of 'attack' contained in the Fourth Geneva Convention in 1949.) There is no non-international armed conflict (NIAC) because the conflict is not sufficiently intense, or because the likely culprit is not an organized armed group. It is far from clear that there has been a 'use of force' as contemplated by Article 2(4) of the Charter, or an 'armed attack' within the meaning of Article 51. Even if the incoming attacks could be attributed to a state, the conflict likely is not an armed conflict. Surely the state must respond to deflect and/or dismantle the sources of the malware, and delaying responses until attribution is certain will greatly exacerbate the crisis.

Although these scenarios do not fully represent the wide range of possible cyber-intrusions that occur now on a daily basis, they do underscore that only the most destructive cyber-attacks fall clearly within the existing international law framework for cyber conflict. What international law principles offer the best options for extending their application more broadly to cyber conflict?

One of the most challenging aspects of regulating cyber war is timely attribution. As Joel Brenner reminds us, 'the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work'.[17] Cyber-attacks also often occur in stages, over time. Infiltration of a system by computers operated by different people in different places may be followed by delivery of the payload and, perhaps at a later time, manifestation of the harmful effects. At what stage has the cyber-attack occurred? Attribution difficulties also reduce the disincentives to cyber-attack and further level the playing field for cyber war waged by terrorists and other non-state actors. Although identifying a cyber-intruder can be aided by a growing set of digital forensic tools, attribution is not always fast or certain, making judgments about who was responsible for the cyber intrusion that harmed the victim state probabilistic.[18] Even where the most sophisticated forensics can reliably determine the source of an attack, the secrecy of those methods may make it difficult to demonstrate attribution in a publicly convincing way. Because the ad bellum justifications for responding to a cyber-attack are tied to attribution of the attack and thus identification of the enemy, the legal requirements for attribution may at least delay effective defenses or responses.

The 'use of force' rubric from Article 2(4) establishes the benchmark standard for determining a violation of international law in the world of kinetic conflict. Once a use of force occurs, permissible responses are determined by the law of state responsibility, potential Security Council resolutions, and the law of self-defense.[19] The traditional and dominant view among member states is that the prohibition on the use of force and right of self-defense apply to armed violence, such as military attacks,[20] and only to interventions that produce physical damage. As such, most

---

[17] Joel F Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press 2011).

[18] W A Owens, K W Dam and H S Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Research Council 2009) §2.4.2: 33–4, 245, 253, 261, 263; S E Goodman and H S Lin (eds), *Toward a Safer and More Secure Cyberspace* (National Research Council 2007).

[19] See Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited *(*2011) 56 Vill L Rev 573–80.

[20] *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (n 14) 253.

cyber-attacks will not violate Article 2(4).[21] Throughout the Cold War, some states argued that the Article 2(4) 'use of force' prohibition should focus not so much on the instrument as the effects of an intrusion and thus forbids coercion, by whatever means, or violations of sovereign boundaries, however carried out.[22] The United States opposed these efforts to broaden the interpretation of 'use of force' by developing states, and by the end of the Cold War Charter interpretation had settled on the traditional and narrower focus on armed violence.[23]

An interpretation of Article 2(4) could evolve to include cyber intrusions, depending on the severity of their impact. State practice may in the future recognize cyber intrusions as 'uses of force', at least when cyber-attacks deliver consequences that resemble those of conventional armed attacks.[24] Public statements by the United States in recent years suggest that the US government is moving toward this sort of effects-based interpretation of the Charter's use of force norm in shaping its cyber-defense policies, a position at odds with the US government's history of resisting flexible standards for interpreting Article 2(4).[25] As historically interpreted, however, the Charter purposefully imposes an additional barrier to a forceful response to a use of force. The response to such a use of force cannot itself rise to the level of use of force unless authorized by the Security Council or is a lawful action in self-defense.[26] In other words, unilateral responses to a use of force are permitted only if the intrusion constitutes an armed attack recognized by Article 51.

---

[21] Jason Barkham, 'Information Warfare and International Law on the "Use of Force"' (2001) 34 NYU J Intl L & Pol 56.

[22] Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale J Intl L 421.

[23] Ibid 431.

[24] *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (n 14) 33–4; Waxman (n 18) 438, citing Abraham D Sofaer et al, 'Cyber Security and International Agreements' in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (2010) 179, 185; Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Colum J Transnatl L 914–15; Oona A Hathaway, 'The Law of Cyber-Attack' (2012) 100 Cal L Rev 848; US White House, *The National Security Strategy of the United States of America* (2010) 22; *Tallinn Manual* (n 6) rule 11.

[25] See Waxman (n 18) 463–7; Ellen Nakashima, 'U.S. Official Says Cyberattacks Can Trigger Self-Defense Rule' *Washington Post*, 18 September 2012.

[26] Vida M Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?' (2005) 51 Naval L Rev 172–4.

Some scholars have argued that cyber-attacks that are especially disruptive but have not been traditionally considered as armed attacks under Article 51 might give rise to the Article 51 right of self-defense.[27] But no international tribunal has so held. In a case involving conventional armed violence, but on a smaller scale, the United States argued unsuccessfully before the ICJ that its naval attacks on Iranian oil platforms was justified by the right of self-defense following low-level Iranian attacks on US vessels in the Persian Gulf.[28] Although the separate opinion of Judge Simma in the *Oil Platforms* case argued that self-defense should permit more forceful countermeasures where the 'armed attack' threshold has not been met,[29] this more flexible approach has not been accepted by the ICJ or any court, and only state practice is likely to change the prevailing traditional interpretation.

In addition, the 'use of force' framework has little value in developing responses to terrorists. By the terms of the Charter, non-state actors cannot violate Article 2(4), and responses to uses of force are limited to actions carried out by or otherwise the responsibility of states.[30] Guidance on the degree of state control that must exist to establish state liability for a non-state group's actions was supplied by the ICJ in the *Nicaragua* case, where the Court limited US responsibility for actions of the Nicaraguan Contras to actions where the United States exercised 'effective control of the military or paramilitary operations [of the Contras] in the course of which the alleged violations were committed'.[31] Only if the state admits its collaboration with terrorists or is otherwise found responsible for the terrorists' actions may the victim state use force against the terrorists and sponsoring state.[32]

The law of self-defense remains unsettled. The text of Article 51—'armed attack'—is not as amenable as 'use of force' to a flexible interpretation. Nor did the Charter drafters consider the possibility that very harmful consequences could follow from a non-kinetic cyber-attack.

---

[27] See Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stan J Intl L 207, 233–9; Schmitt (n 20) 930–4; *Tallinn Manual* (n 6) rule 13.

[28] *Iran v US,* 161 ICJ Rep paras 12, 46–7 (2003).

[29] Ibid.

[30] UN International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), UN GAOR, 53rd Sess. Supp. No. 10, at 80, UN Doc A/56/20, Article 8.

[31] *Nicaragua v US*, 14 ICJ Rep (1986) paras 115, 109; *Prosecutor v Tadić*, ICTY Appeals Chamber Judgment (1999) para 145.

[32] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (n 26).

Nonetheless, outside the cyber realm, state practice has evolved toward accepting that attacks by terrorists may constitute an armed attack that triggers Article 51 self-defense.[33] The text of Article 51 does not limit armed attacks to actions carried out by states, although the state-centric model of the Charter strongly suggests that the drafters contemplated only those armed attacks by non-state actors that could be attributed to a state as Article 51 armed attacks.

The dramatic development that made it clear that armed attacks may occur by non-state terrorists regardless of the role of a state was 9/11. Within days of the attacks, the Security Council unanimously passed Resolutions 1368 and 1373 and recognized 'the inherent right of individual or collective self-defense in accordance with the Charter' in responding to the attacks.[34] NATO adopted a similarly worded resolution.[35] Unlike prior instances where non-state attackers were closely linked to state support, the Taliban merely provided sanctuary to Al-Qaeda and did not exercise control and were not substantially involved in Al-Qaeda operations.[36]

State practice in the international community supported extending self-defense as the ad bellum justification for countering Al-Qaeda on a number of occasions since 2001.[37] While the ICJ has not ratified the evolving state practice, and even seemed to repudiate it in at least three decisions—twice since 9/11 (*Nicaragua v US* in 1986, *Democratic Republic of the Congo v Uganda* in 2005, and *Wall Advisory Opinion* in

---

[33] Steven R Ratner, 'Self-Defense Against Terrorists: The Meaning of Armed Attack' in N Schrijver and L van den Herik (eds), *The Leiden Policy Recommendations on Counter-Terrorism and International Law* (2012) 5–6, 8–9; Michael N Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (National Academies Press 2010) 151, 163–4; Michael N Schmitt, 'Responding to Transnational Terrorism under the *Jus Ad Bellum*: A Normative Framework' (2008) 56 Naval L Rev 18-19; Sean Watts, 'Low-Intensity Computer Network Attack and Self-Defense' (2011) 87 Intl L Stud 60-61; Dept. of Defense Office of Gen. Counsel 1999; *Tallinn Manual* (n 6) rule 13.

[34] Security Council Resolution 1368 (2001), UN Doc S/RES/1368; Security Council Resolution 1373 (2001), UN Doc S/RES/1373.

[35] North Atlantic Treaty Organization (2001), *Statement by the North Atlantic Council*, accessed 4 May 2017 at http://www.nato.int/docu/pr/2001/p01-124e.htm.

[36] See Derek Jinks, 'State Responsibility for the Act of Private Armed Groups' (2003) 4 Chi J Intl L 89.

[37] Ratner (n 29).

2004)—the trend is to accept the extension of armed attack self-defense authorities when non-state groups are responsible, provided the armed attack predicate is met and the group is organized and not an isolated set of individuals. In general, states that were victimized by non-state terrorist attacks were more likely to advocate the more expansive conception of self-defense. Unsurprisingly, the US Department of Defense supports the same position.[38] Thus, despite the apparent gulf between the text of the Charter as interpreted by the ICJ and state practice, whether an 'armed attack' is kinetic or cyber-based, armed force may be used in response to an imminent attack if it reasonably appears that a failure to act promptly will deprive the victim state of the opportunity to defend itself.[39]

The legal bases for self-defense may also be extended to anticipatory self-defense in the cyber context. As evolved from Secretary of State Daniel Webster's famous formulation in response to the *Caroline* incident that self-defense applies in advance of an actual attack when 'the necessity of that self-defense is instant, overwhelming, and leaving no moment for deliberation',[40] contemporary anticipatory self-defense permits the use of force in anticipation of attacks that are imminent, even if the exact time and place of attack are not known.[41] Imminence in contemporary contexts is measured by reference to a point in time where the state must act defensively before it becomes too late.[42] In addition to imminence or immediacy, the use of force in self-defense must be necessary—law enforcement or other non-use of force means will not suffice—and the attacking group must be shown to have the intent and means to carry out the attack.[43]

In contemporary state practice, nearly every use of force around the world is justified as an exercise of self-defense.[44] As Sean Watts has observed, 'in the post-Charter world … states have resurrected pre-Charter notions that self-defense includes all means necessary for self-preservation against all threats'.[45] So interpreted, the legal parameters of self-defense law may be adapted to cyber-attacks, subject to meeting the

---

38 Ibid.
39 Schmitt (n 15) 593.
40 Daniel Webster, 'Letter', reprinted in H Miller (ed), *Treaties and Other International Acts of the United States of America*, *Vol 4* (1934) (1842).
41 *The National Security Strategy of the United States of America* (n 20).
42 See Schmitt 2008 (n 29) 18–19; *Tallinn Manual* (n 6) rule 15.
43 See Schmitt 2008 (n 29) 18–19.
44 Watts (n 29).
45 Ibid 76.

formidable Article 51 threshold of armed attack. Thus, if a cyber-attack by a non-state actor constitutes an armed attack as contemplated by the Charter, self-defense allows the victim state to conduct forceful operations in the state where the terrorist perpetrators are located if that state is unwilling or unable to police its territory.[46] In the sphere of anticipatory self-defense, the fact that cyber-attacks arrive unattributed and without warning provide strong analogs to the challenges of counter-terrorism law that give rise to the contemporary interpretation. At the same time, even though reliance on self-defense arguments is and will remain tempting in the cyber arena, the Charter system remains subject to the 'armed attack' qualification.

What does international law say about cyber-attacks that do not meet the armed attack threshold? One potentially important rule distilled from the Charter and state practice is that a number of small cyber attacks that do not individually qualify as armed attacks might do so when aggregated, provided there is convincing evidence that the same intruder is responsible for all of the attacks.[47] The so-called 'pin-prick' theory could have emerging importance in supporting cyber self-defense, especially if technical advances aid in attribution. Otherwise, distilling the conclusions developed in this section so far, the international law of self-defense may only justify responses to cyber-attacks that are sufficiently destructive to meet the armed attack threshold.

What international law determines the permissible responses to a cyber-attack that causes significant economic harm but no physical damage? Is the loss or destruction of property sufficient to trigger a kinetic response? The answer turns in part on whether the state wishes to use force in response. For non-forceful responses, customary international law has long allowed countermeasures—temporarily lawful actions undertaken by an injured state in response to another state's internationally unlawful conduct.[48] The state that places malware inside the cyber systems in another state has violated the victim state's sovereignty. In the cyber context, sovereignty intrusions that fall short of armed attacks as defined by the Charter are nonetheless in violation of the international law norm of non-intervention and thus permit the reciprocal form of violation by the victimized state. As codified by the

[46] Ashley S Deeks, 'Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense' (2012) 52 Va J Intl L 483.

[47] *Tallinn Manual* (n 6) rule 13.

[48] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (n 26).

UN International Law Commission's Draft Articles on State Responsibility for Internationally Wrongful Acts, countermeasures must be targeted at *the state* responsible for the prior wrongful act, and must be temporary and instrumentally directed to induce the responsible s*tate* to cease its violation.[49]

In the cyber arena, one important question is whether countermeasures include active defenses, 'hack backs' which attempt through an in-kind response to disable the source of an attack while it is underway.[50] Whatever active defense technique pursued by the victim state thus has a reciprocal relationship with the original cyber-intrusion, and like the original intrusion the active defense presumptively breaches state sovereignty and violates the international law norm of non-intervention. (Passive defenses, such as firewalls, attempt to repel an incoming cyber-attack.) Active defenses may be pre-set to deploy automatically in the event of a cyber-attack, or they may be managed manually.[51] Computer programs that relay destructive viruses to the original intruder's computer or packet-flood the computer have been publicly discussed.[52] Although descriptions of most active defenses are classified, the United States has publicly stated that it employs 'active cyber defense' to 'detect and stop malicious activity before it can affect [Department of Defense] networks and systems'.[53]

In theory, countermeasures provide a potentially effective defensive counter to many cyber-attacks. In practice, a few problems significantly limit their effectiveness. First, the Draft Articles codify customary law requirements that before a state may use active defense countermeasures it must find that an internationally wrongful act caused the state harm, identify the state responsible, and follow various procedural requirements, delaying execution of the active defense.[54] The delay may be exacerbated by the problems in determining attribution. Second, countermeasures customarily are available in state-on-state conflicts, not in response to intrusions by a non-state actor. A non-state actor's actions may be attributable to a state when the state knows of the non-state actors' actions and aids them in some way,[55] or possibly when the state

---

[49] Ibid Article 49.
[50] Jensen (n 23) 230.
[51] Ibid 231.
[52] Ibid.
[53] US Dept of Defense, *Strategy for Operating in Cyberspace 7* (2011) 230.
[54] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (n 26) Articles 49–52.
[55] Ibid Article 16.

merely knowingly lets its territory be used for unlawful acts.[56] In most instances, however, international law supplies no guidance on countermeasures that respond to intrusions by non-state actors. Third, the normative principle that justifies countermeasures is that the initial attacker must find the countermeasure sufficiently costly to incentivize lawful behavior. For non-state groups that act independently of any state, a fairly simple relocation of their servers or other equipment may evade or overcome the countermeasures and remove any incentives to stop the attacks. In sum, although the countermeasures doctrine is well-suited to non-kinetic responses to cyber-attacks by states, attribution delays may limit their availability, and the line between permitted countermeasures and a countermeasure that constitutes a forbidden 'use of force' is not clear. Nor do countermeasures apply in responding to an attacker unaffiliated with any state.

Even if each of these limitations is overcome, the prevailing view is that active defenses may only be employed when the intrusion suffered by a victim state involves a 'use of force' as interpreted at international law.[57] Taken together, the promise of countermeasures in responding to cyber-attacks is significantly compromised by problems of attribution, timing, efficacy and logic. However, if active defense countermeasures do not involve a 'use of force', the attribution problem loses its urgency. There is no clear international barrier to non-use of force countermeasures, and attribution may be determined when feasible since no force is being used. Finally, the International Group of Experts that prepared the *Tallinn Manual* acknowledged that while victim states may not continue countermeasures after the initial intrusion had ended, state practice 'is not fully in accord … States sometimes appear motivated by punitive considerations … after the other State's violation of international law had ended'.[58] In other words, customary law on cyber countermeasures is in flux.

Whether the development of cyber-law so removed from the text of the Charter represents the optimal path forward for the law of cyber-conflict is unclear. On the one hand, the Charter's traditional self-defense doctrine may not leave states sufficient authority to respond to the full range of cyber threats they face. On the other hand, the development of customary

---

[56] *UK v Albania,* 4 ICJ Rep 22 (1949); 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' (2009) 210 Mil L Rev 1, 43.

[57] Jensen (n 23) 231.

[58] *Tallinn Manual* (n 6) rule 9.

law through state practice is the ultimate flexible vehicle for making new law to confront emerging problems. As with other aspects of norm development in international law, many states with vested interests in applying norms from the kinetic warfare realm to cyber tend to favor retaining core Charter principles, while states more often victimized by terrorism have looked to state practice to develop customary law norms. In any case, even Charter law interpreted at degrees of separation from the Charter is preferable to a legal vacuum.[59]

3. DEVELOPING CONTEMPORARY AD BELLUM PRINCIPLES FOR CYBER CONFLICT BELOW THE ARMED CONFLICT THRESHOLD

Particularly for cyber-attacks that are especially disruptive but not destructive—intrusions that may be increasingly pervasive, operating beneath the radar of many states' existing defensive mechanisms, and capable of fairly easily and cheaply being perpetrated by virtually any state or non-state actor—the Charter provides an incomplete normative blueprint. The asymmetric opportunities for state and non-state adversaries abound, and under the Charter norms victim states may have to choose between defending themselves unlawfully and absorbing continuing cyber-attacks.[60] Alternately, arguing that the measure of compliance with the gateway articles of the Charter should be practical, based on the effects of a cross-border intrusion and not on the nature of the instruments that cause the effects, Michael Schmitt and other scholars have argued that cyber-attacks that cause significant harm should count as uses of force and, less plausibly, armed attacks. Their view is that once the gateway determinations are made for the Charter to reach the cyber domain, international law supplies at least a serviceable roadmap for limiting cyber-war. The debates continue as the daily tally of cyber-attacks escalates.

This chapter has shown that arguments to apply the 'use of force' and 'armed attack' Charter categories to cyber may be based on a tautology; if the incoming cyber intrusion is construed as an armed attack, the victim state may respond in kind. If not so construed, the same or a

[59] Watts (n 29) 66.
[60] Ibid 60–61.

similar response may not be considered an armed attack.[61] The fact that it may be possible simply to characterize a new form of intrusion as a use of force or armed attack is not satisfying analytically and, over time, such tautological reasoning may diminish the normative values embedded in these critical cornerstones of the Charter. In a similar vein, state practice in shaping responses to cyber-intrusions has been characterized as applying a 'know it when you see it'[62] approach to deciding when the intrusion constitutes a 'use of force' or 'armed attack' that would trigger IHL requirements. Such ad hoc reasoning does little to build confidence that the international community may arrive at acceptable norms for protecting critical infrastructure from cyber threats.

Meanwhile, the dynamic growth of reliance on the Internet to support our infrastructure and national security have caused the United States to modify its longstanding views on the predicates for treating a cyber-intrusion as an 'armed attack' or 'use of force'. As Matt Waxman has noted, US government statements suggest that cyber-attacks that have especially harmful effects will be treated as armed attacks, while lower level intrusions would enable cyber countermeasures in self-defense.[63] The result is a tiered interpretation of Article 51 based on the instrument of attack—an expansive interpretation when defending against armed violence, and a narrower view with a high impact threshold for cyber-attacks.[64] Whatever precision and calibration of authorities is gained by these fresh reinterpretations of the Charter, they replace the relative clarity of an 'armed attack' criterion with fuzzier effects-based decision-making that injects ever more subjectivity and less predictability into future self-defense projections. Taking into account the characteristics of cyber conflict—uncertainty, secrecy and lack of attribution—finding consensus on international regulation through these Charter norms will be a tall order.[65]

Attribution of cyber-attacks is a technical problem, not one that the law can fix. Yet the challenges in attributing intrusions in real time with confidence should not foreclose the development of legal authorities that protect national and human security. Anonymity and surprise have long been central tenets of terrorist attacks, and international law has developed normative principles, including anticipatory self-defense, that

---

[61] Dept of Defense Office of Gen Counsel, *An Assessment of International Legal Issues in Information Operations* (1999) 16–19.

[62] *Jacobellis v Ohio*, 378 US 197 (1964) (Stewart J, concurring).

[63] Waxman (n 18) 439.

[64] Ibid.

[65] Ibid 443.

accommodate these characteristics. By analogy international law may develop along similar lines to provide ad bellum bases for responding to cyber-attacks. In light of continuing attribution problems, and the likelihood that cyber-attacks will come from sources around the world, a cyber-international law could subordinate traditional legal protections that attach to national boundaries and narrowly tailor mechanisms that permit defending against the sources of the attacks, whatever their locations.

One of the difficulties of attribution is that learning that an attack comes from within a certain state does not tell us whether the attack is state-sponsored or was carried out by a non-state actor. Existing Charter and IHL law of state responsibility—heavily influenced by the United States and other western states that do not have comprehensive controls over private infrastructure—does not make the state responsible for the actions of private actors over which it has no direction or control. There is thus no clear IHL or Charter-based authority to go after the private attackers inside a state when that state was not involved in the attacks.[66] International law offers an alternative normative path. For example, criteria could be developed that indicate the circumstances where absolute attribution may be delayed in favor of immediate defensive action, when intelligence is reliable enough to authorize those actions, and under which circumstances defensive operations may invade territorial sovereignty without state permission.

The 2011 US *International Strategy for Cyberspace* asserts that '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'.[67] Because cyberspace has been around for a relatively short period of time, there is no extensive catalog of state practice that provides the basis for a body of customary cyber conflict law. Further complicating the search for evidence of customary law in cyber conflict is the secrecy that surrounds most cyber operations, and their lack of attribution.[68] In the last decade, however, several mostly public cyber-attacks occurred, including those in Estonia (2007), Georgia (2008), and the first in an escalating series of attacks on US military, Intelligence Community, and commercial networks for the purpose of transferring sensitive

[66] *Tallinn Manual* (n 6) rule 6.

[67] Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) Strategic Studies Q 126, 140.

[68] Ibid.

information or stealing intellectual property. By 2010, the Stuxnet worm had targeted Iranian nuclear facilities, although the attack was not publicly revealed until 2012. Surprisingly, Iran did not blame Stuxnet or even a cyber-attack by the United States or Israel for the delays in making its nuclear plant operational. (It surely would have responded if a missile had damaged its facilities.) In any case, Iran did not allege a violation of international law by cyber means in the Stuxnet episode.

The Russian cyber-attacks against Georgia in 2008 likewise did not clearly constitute a case of a purely cyber conflict waged by one state against another. Russian troops crossed the border as an invasion force on the same day that Russian cyber actions were taken, most likely to interfere with Georgia's communications during the surprise armed attack by the Russian military. Georgia then declared it was in a state of war with Russia, but it did not single out the cyber intrusions as an attack.[69] Likewise, the Estonian intrusions by Russia in 2007 involved distributed denial of service activities, more like a series of criminal acts than a use of force. A further complication in Estonia was the inability to clearly attribute the denial of service intrusions.

As these examples show, customary international law governing cyber conflict is likely to develop unevenly over time, as state, regional and perhaps even global policies and practices evolve. Consider one example. Intelligence collection is practiced by every state. While the domestic laws of nearly every state forbid spying within its territory, neither those laws nor any international law purports to regulate espionage internationally. In the digital world, the equivalent intelligence collection activity is cyber-exploitation—espionage by computer, a keystroke monitor, for example—and nothing in the Charter, IHL, or other customary law traditionally stands in its way, except to the extent that espionage involving military weapons systems constitutes armed aggression.[70] Given the growing capabilities of digital devices to spy, exploit and steal, including military and other sensitive national secrets, the absence of international regulation is problematic. It is possible that IHL could develop customarily through state practice to recognize legal limits on one variant of cyber-exploitation where the software agent is capable of destructive action or may facilitate the same.[71] For example, malware has infiltrated and interfered with the oil and gas, freight and passenger rail

[69] Ibid.

[70] Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 A F L Rev 223–4.

[71] National Research Council 2009 (n 14) 261, 263.

signaling systems,[72] and the US air traffic control system is vulnerable to cyber-attack.[73]

International law for cyber-operations could evolve through something like natural law-type or just war theory reasoning, as has been the case with development of some other international law norms.[74] Just war theory and natural law reasoning or its equivalent has served as a gap-filler in international law, and could do so for cyber. The making of customary international law is often unilateral in the beginning, followed by a sort of dialectic of claims and counterclaims that eventually produce customary law that is practiced by states.[75] As some prominent US academics developed theories of 'vertical domestication'[76] to encourage greater respect and adherence to international law by the US government, in the last decade the US government sought to export its emerging counterterrorism law as international law in response to kinetic attacks on the United States and its interests. Although controversy surrounded some of the US government policies and practices, counterterrorism law has matured and developed normative content around some of its revised tenets, such as the permissible use of force against non-state terrorists inside a sovereign state.[77]

However it occurs, international law norm development for cyber might expand or contract the authorities that would otherwise govern under current interpretations of the Charter. On the one hand, an evolving international law regime may enable victim states more tools and greater flexibility in anticipating and responding to cyber-attacks. Active defense countermeasures and other kinds of responses may be permitted, through state practice, but predicated upon legal authority, where the same responses would not have been lawful under the Charter as traditionally

---

[72] Brenner (n 13) 105–10.

[73] US General Accounting Office, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems,* GA0-15-221 (2015).

[74] Jeffrey L Dunoff and Mark A Pollack, 'What Can International Relations Learn From International Law?' (2012) Temp Univ Legal Stud 11.

[75] Michael W Reisman, 'Assessing Claims to Revise the Laws of War' (2003) 97 Am J Intll L 82.

[76] Harold H Koh, 'The 1998 Frankel Lecture: Bringing International Law Home' (1998) 35 Hous L Rev 626–7; Harold H Koh, 'Transnational Legal Process' (1996) 75 Neb L Rev 181, 183–4.

[77] Robert M Chesney, 'Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force' (2011) 13 Y B Intl Hum L 3; James B Steinberg and Miriam R Estrin, 'Harmonizing Policy and Principle: A Hybrid Model for Counterterrorism' (2014) 7 J Natl Sec L & Poly 161.

interpreted because the armed attack threshold was not met. On the other hand, some cyber responses that are now lawful under international law because there is no use of force or armed attack involved in the response—a small scale action designed to neutralize an incoming cyber-intrusion aimed at one system, for example—could be considered unlawful if the harmful consequences are significant.[78]

For the United States, the fact that so much of the infrastructure is privately owned makes securing the infrastructure legally and practically problematic,[79] and yet heavy reliance on networked information technology makes the United States highly vulnerable to cyber-intrusions. The government's recent posture on cyber operations has been to mark out preferred clear positions on the authority to respond to destructive cyber-attacks with armed or forceful responses, while maintaining what Matt Waxman aptly calls 'some permissive haziness'[80] concerning the norms for responding to cyber-intrusions that are less harmful but distracting. From the domestic perspective, the United States can assure itself of the authority to respond to serious intrusions while preserving the flexibility to tailor its countermeasures and develop its cyber defenses according to the nature and severity of the threat faced.

The nuanced calculations by the United States in developing its cyber doctrine are consistent with its longstanding opposition to some other states' expansive interpretations of Articles 2(4) and 51 to include economic coercion and political subversion.[81] Yet emerging cyber doctrine by the United States may be seen in the international community as just the sort of proposed expansion of the Charter norms that the United States has publicly opposed in the past. Indeed, as the evolving criteria for what triggers the Article 51 right of self-defense over the last 25 years shows, freighting fast-developing cyber-defense norms onto an already-burdened Article 51 invites controversy and may destabilize and even undermine the normative value of the Charter.

In activating the US Cyber Command in 2010, the Department of Defense confronted congressional skepticism and challenges from across the political spectrum that focused on fears of the Command's capabilities for interfering with the privacy rights of citizens, the policies and authorities that would define its mission, and its relationship to the

78 National Research Council 2009 (n 14) 245.
79 Waxman (n 18) 451.
80 Ibid 452.
81 Ibid 453.

nation's largely privately held critical infrastructure.[82] Against this backdrop, from the beginning Cyber Command and the Department of Defense have stated that existing Charter interpretations and the laws of war adequately provide the authorities needed to defend the United States from cyber-attack.[83] Even as President Obama in 2013 issued a classified policy directive that detailed basic principles for US responses to cyber intrusions (PPD-20 2013), including defensive and offensive cyber operations, the Legal Adviser to the State Department continued to affirm that the United States would engage in cyber-conflict according to existing understandings of international law.[84]

In 2015, the US Department of Defense publicly announced two major cyber milestones. First, in April, the *Department of Defense Cyber Strategy* stated that 'DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence … [which] may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States'.[85] As a statement of US government policy, note the subtle but unmistakable shift away from the 'armed attack' and 'use of force' categories. Seriously adverse foreign policy or economic impacts may occur absent kinetic attacks, by cyber means. The *Strategy* also reiterates that 'the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property … in a way that reflects enduring U.S. values, including support for the rule of law, as well as respect and protection of the freedom of expression and privacy, the free flow of information, commerce, and ideas'.[86] These additional cornerstone principles are important in limiting US cyber operations and in setting an example for other states as they shape their cyber policies. Other than a reminder that DoD cyber operations are conducted 'in accordance with the law of armed conflict', the *Strategy* does not indicate that the new characterization of the DoD cyber mission is based on legal obligation. Still, if practiced through publicly acknowledged cyber actions over some

---

[82] Ellen Nakashima, 'Cyber Command Chief Says Military Computer Networks Are Vulnerable' *Washington Post* (4 June 2010).

[83] Watts (n 29).

[84] Harold H Koh, 'International Law in Cyberspace: Remarks Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference' (2012) 54 Harv Intl L J Online 3.

[85] *The Department of Defense Cyber Strategy* (n 4).

[86] Ibid.

period of years, the DoD formulation could provide a pillar of a normative architecture for cyber conflict.

To its credit, the 2015 *Strategy* suggests that developing cyber doctrine may be more effective and more likely to be accepted internationally if it is separated from the effects-based approach relied upon by the Charter and IHL-based doctrines for cyber-operations. Not that such a legal code of conduct based in international law would be a panacea. Law must follow, not lead, particularly in an area like cyber, where policies are not yet well defined and strategies are unclear.[87]

Second, in June 2015, the Department of Defense released its long-awaited *Law of War Manual*.[88] For the first time, DoD included a chapter on cyber operations. In general, the *Manual* anticipates that cyber-attacks that cause physical damage will be subject to the rules governing kinetic attacks.[89] The *Manual* also recognizes that cyber operations may constitute 'use of force' under the Charter, based on the effects of the cyber intrusion,[90] and that the Article 51 right of self-defense applies to a use of force or armed attack,[91] whether the attack is attributed to another state or to a non-state actor.[92] In other words, the *Manual* lags behind the *Strategy* and simply superimposes ad bellum principles from kinetic armed conflict on cyber operations. Follow but not lead, indeed.

4. CONCLUSIONS

Imagine this scenario. It is summertime in the not-distant future. Just before the afternoon rush hour on a hot and steamy July day, the northeastern United States is hit with a massive blackout. The electric grid is crippled from Boston to New York, Philadelphia to Baltimore and Washington, and from there west as far as Cleveland. While back-up generators resume the most critical operations in hospitals and other critical care centers, all other activities that depend on electricity come to a sudden halt.

Government and private industrial security experts quickly discover the software and malware that has accessed supervisory control and data

[87] Waxman (n 18) 455–7.
[88] US Dept of Defense, *Law of War Manual* (2015).
[89] Ibid 16.2.
[90] Ibid 16.3.1.
[91] Ibid 16.3.3.1.
[92] Ibid 16.3.3.4.

acquisition (SCADA) controls—the industrial control system that supervises data over dispersed components of the electric grid and which are connected to the global Internet.[93] In recent years, industry reports that a few laptops containing information on how to access SCADA controls were stolen from utility companies in the Midwest. During the same period, computers seized from Al-Qaeda and IS captives abroad contained similar details about US SCADA systems. The vast majority of the affected electric grid is privately owned, and officials estimate that the cyber-attacks have done long-term damage to critical system components, and have rendered useless generators and other equipment that must be replaced where no back-up replacement equipment is standing by. Even rudimentary repairs will take weeks or months, and full system capabilities may not be restored for more than one year. Economic losses will be in the billions of dollars, and millions of Americans' lives will be disrupted for a long time.

The software and malware were set to trigger the blackout at a pre-determined time. The attacks were not attributed, and although intelligence and law enforcement experts quickly traced the original dissemination of the attacks to computers in South Asia, the only other available intelligence comes from the seized and stolen laptops. The governments of Russia, China and Iran have denied any involvement in the attacks, and no intelligence points to their involvement. Al-Qaeda and IS have shown interest in cyber capabilities, and the seized laptops suggest that some steps were taken to acquire them.

Assuming that the United States concludes that terrorists are most likely behind the attacks, what law governs the response? If, instead, we decide that the attacks were launched by Russian intelligence operatives situated in South Asia, what law applies? This chapter has helped draw attention to the incompleteness of the legal regime that will be required to provide the normative justifications in international law for responding to these intrusions.

The stakes are escalating. The United States used offensive cyber weapons to target Iran's nuclear program, and states and non-state actors are increasingly aware that cyber weapons—offensive and defensive—are available, with ever-growing sophistication. Although reports indicated the United States declined to use cyber weapons to disrupt and disable the Qaddafi government's air defense system in Libya at the start of the US/NATO military operation in 2011 because of the fear that such a cyber-attack might set a precedent for other nations to carry out their own

[93] Brenner (n 13) 96–7.

offensive cyber-attacks,[94] Stuxnet created the precedent, as did Israel's cyber-attack on Syrian air defenses when it attacked a suspected Syrian nuclear site in 2007,[95] Russia's cyber-attacks in its dispute with Georgia,[96] and the apparent use of cyber-weapons by the United States to target Al-Qaeda websites and terrorists' cell phones.[97] Now that the cyber war battlefield apparently has expanded to Beirut banks and a neutral state (Lebanon),[98] it appears that cyber weapons are being used beyond countering imminent national security and infrastructure threats.

Developing an international consensus on the norms for cyber conflict will not be easy. The state of doctrinal international law is only partly to blame. At least as important as constraints are the political differences among states and non-state actors in shaping cyber norms. In addition, the facts needed to make the normative judgments in this fast-paced realm of changing technologies are now and will be for the foreseeable future hard to come by and even more difficult to verify.[99] Law will play catch up, as it should, but the lag between evolving technologies and normative stability in cyber operations may be a long one. Legal change will occur, to be sure, but the process may be fraught.

This chapter has shown that the international community runs significant risks in continuing to build cyber-conflict law using the Charter/IHL model. One overarching concern is that categorizing cyber-attacks as a form of armed attack or use of force may enhance the chance that a cyber-exchange could escalate to a military conflict.[100] If, over time, the thresholds for what constitutes an armed attack are lowered to reach more forms of cyber-intrusion, legal barriers to military force will be lowered, leading to more military conflicts in more places. The high threshold for invoking the Charter's self-defense authorities traditionally supported by

---

[94] Eric Schmitt and Thom Shanker, 'U.S. Debated Cyberwarfare in Attack Plan on Libya' New York Times (17 October 2011).

[95] Dave A Fulghum and Robert Wall, 'Cyber-Combat's First Shot: Attack on Syria Shows Israel is Master of the High-Tech Battle' (2007) Aviation Week & Space Technology 28.

[96] John Markoff, 'Before the Gunfire, Cyberattacks' *New York Times* (12 August 2008).

[97] Markoff (n 92); Jack Goldsmith, 'Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya' Lawfare (18 October 2011).

[98] Katherine Mayer, 'Did the Bounds of Cyber War Just Expand to Banks and Neutral States?' *The Atlantic* (17 August 2012).

[99] Waxman (n 18) 448.

[100] Martin C Libicki, *Cyberdeterrence and Cyberwar* (RAND 2009) 69–70; Mary Ellen O'Connell, 'Cyber Security Without Cyber War' (2012) 17 J Conflict & Sec L 187, 190–91, 199.

the United States also offers some insurance against precipitous action in response to unattributed cyber-attacks. That such a high threshold fails to deter low-level hostilities may be a reasonable price to pay.[101]

Yet the high self-defense threshold also leaves unregulated a wide swath of cyber-intrusion techniques, those now in existence and others yet to be invented. This byproduct of the bifurcation of international law into war and peace, armed conflict or not armed conflict, armed attack and use of force or not leaves every intrusion that fails to meet the kinetic standard not subject to international law limitations, except for the limited customary authorities for countermeasures and the open-ended rule of necessity.[102] If states or the international community attempt to further expand the reach of self-defense and IHL in idiosyncratic ways to non-destructive cyber intrusions, the Charter and IHL will be compromised.

Despite the disconnect between the text of the Charter as interpreted by the ICJ and state practice, whether an attack is kinetic or cyber-based, state practice has been to enable armed force in response to an imminent attack if it reasonably appears that a failure to act promptly will deprive the victim state of the opportunity to defend itself. Article 51, or at least its self-defense shadow, has become the go-to authority for military action waged by states, whatever the context. The self-defense arguments may be adapted to cyber, but the further the analogies to responses to armed attacks stray from kinetic means, the greater the likelihood that Article 51 norms will erode. The temptation to rely on Article 51 is great, to be sure, particularly where, as in cyber, other sources of legal authority to take what is viewed as essential defensive action may not exist.

[101] Waxman (n 18) 446–47.
[102] *Tallinn Manual* (n 6) rule 9.