14. An emerging international legal architecture for cyber conflict

William C. Banks[1]

Assume that senior government ministers meeting to discuss economic policies at the capital in a major industrial State are interrupted by an assistant who reports that large scale malware programs have infected the critical infrastructure of the State and its private sector. In the security sector, large-scale routers throughout the network are failing, and classified systems have been penetrated. As the ministerial meeting suddenly shifts its attention to the fast-spreading cyber-intrusion, the malware continues to spread, causing Internet-based systems to fail throughout the country. Government and financial institutions continue to be besieged by a distributed denial-of-service attack from tens of thousands of computers organized into botnets – a slang term for the tool that enslaves the computers of unknowing victims. Banks were forced to shut down, incoming payments due from abroad could not arrive, and government ministries closed up shop. Credit card companies shut down their networks worldwide, fearing the spread of the attacks. Meanwhile, the national government closed all its electronic borders. There was as yet no physical damage and no deaths or injuries attributable to the cyber-attacks, but the economic and social costs were high and mounting.

As the government's security, intelligence and law enforcement resources scrambled to identify the source of the attacks and implement defensive measures, legal advisors faced their own challenges. The first intelligence reports showed the sources of the attack coming from computers all over the world, but with no clear indications of any State sponsorship or involvement. Meanwhile, terrorist groups opposed to certain of the victim State government's policies have threatened attacks, but as yet the attacks cannot be clearly attributed. What body of law applies in responding to the attacks? Is the nation at war? If so, who is the enemy? Has there been a 'use of force' or 'armed attack' sufficient to trigger self-defense prerogatives under the UN Charter? Do the attacks create an 'armed conflict' between the State and the as yet unidentified

[1] The author is grateful to Kyle Lundin for excellent research assistance.

enemy and, if so, do the laws of armed conflict (LOAC) apply? What is the source of the legal authority to respond defensively if the perpetrators are non-State terrorists? If the computers responsible for spreading the malware can be identified, but at this time not the State or non-State group perpetrating the attacks, what is the nature and scope of the authority to respond?

This vignette illustrates some of the challenging international law questions that arise in cyber conflict. In this chapter, the focus is on *legal change.* When the normative framework governing kinetic warfare does not fit cyber conflict, how do adaptations occur that permit regulation of or responses to harmful cyber intrusions? In other words, the most important stage of governance in managing cyber conflict has arrived long after the norms and institutions are in place. In setting up legal change in the cyber domain, I will review the *ad bellum* justifications for conducting cyber war within the Charter and LOAC systems. As highlighted by the framing chapter for this volume, I show that political considerations have significantly impacted the process for the changing norms of cyber war governance, and that political interests of different state actors have often served to obstruct or at least slow down agreement on core cyber norms. I also conclude that the Charter and LOAC provide insufficiently clear legal guidance, and that further accommodating the various forms of cyber war could compromise the normative integrity of the existing system for limiting the use of force and may unnecessarily further militarize the cyber domain.[2] Instead, the core component of the framework for regulating the use of force – the UN Charter – is less important in developing future prescriptions than is customary international law, often revealed through state practice. Indeed, cyber norms and regulations are evolving in varying ways *across a range of governmental systems*, from the Charter, LOAC, international human rights law and the prescriptions of the World Trade Organization, to domestic law in many states.

The prospect of cyber war has evolved from science fiction and over-the-top doomsday depictions on television, films and novels to reality and front page news. The revelations that the Stuxnet attack on the computers that run Iran's nuclear enrichment program was part of a larger 'Olympic Games' campaign of cyber war begun in 2006 during the George W. Bush administration by the United States and perhaps Israel opened our eyes to the practical reality that the United States is engaged

[2] Mary Ellen O'Connell, 'Cyber Security Without Cyber War' (2012) 17 Journal of Conflict and Security Law 187.

in some kind of cyber-war against Iran. The United States' use of cyber-weapons to attack a State's infrastructure became the first known use of computer code to effect physical destruction of equipment – in this case Iranian centrifuges – instead of disabling computers or stealing data.[3] If the United States can so target Iran's nuclear program, why not go after the North Koreans'? Or the Assad regime in Syria, the Chinese military or Al-Qaeda's global operations? If the United States can achieve important national security and foreign policy objectives through the use of cyber-weapons, can there be any doubt that the United States is now the target of the same kinds of weapons?

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', a categorization that excludes most though not all cyber-attacks.[4] Despite the growing role of the cyber domain in the security sectors of many governments over the last decade, the maturing legal architecture for cyber-war pays little attention to cyber-attacks by terrorists or 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.[5] The resulting *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*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'.[6] The *Tallinn Manual* experts concluded that cyber-attacks can constitute terrorism, but only where the attack has been conducted through 'acts of violence'.[7] In defining the scope of their project, the *Tallinn Manual* experts considered only those forms of cyber-attack that meet the UN Charter and LOAC conceptions

---

[3] David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran' *The New York Times* (Washington, 1 June 2012), accessed 19 September 2016 at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Broadway Paperbacks 2012).

[4] Jelena Pejic, 'Armed Conflict and Terrorism: There Is a (Big) Difference' in Katja Samuel, Ana María Salinas de Frías and Nigel White (eds), *Counter-Terrorism: International Law and Practice* (Oxford University Press 2012).

[5] International Group of Experts, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

[6] ibid Rule 36.

[7] ibid Rules 30, 36.

of 'use of force' or 'armed attack'.[8] In other words, the *Tallinn Manual* concludes that international law proscribes only violent terrorism and thus leaves unregulated an entire range of very disruptive cyber intrusions.[9] To date there has been little attention given to the possibility that new norms embedded in international law could and should supplement existing international law governing cyber war where the intrusions do not meet the traditional kinetic thresholds.

Developing a consensus understanding of the international law of cyber war 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 in the UN Charter and laws of armed conflict – the line between offense and defense – is elusive, particularly taking into account the possibilities afforded by cyber 'active defenses'. 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? In addition, 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?

Even if the technical difficulties in attributing a cyber attack are solved eventually, the differing resources and capabilities of states in the cyber domain manifest themselves as political disputes that further stand in the way of consensus on what rules to support. States with advanced cyber resources may be more willing to favor a norm that assumes attribution on the basis of some technical determinations, for example. States that have vulnerable infrastructure but limited cyber defenses might insist on harder evidence of a cyber intrusion.

Even with these limitations, there may be emerging legal clarity in some cyber-war situations. In instances where a cyber-attack causes physical destruction and/or casualties at a significant level, a cyber-intrusion may constitute an 'armed attack' in UN Charter terms. In these extreme circumstances, even where the attacker is a State-sponsored non-State actor, there is emerging post-11 September customary law

[8] ibid Rule 18.
[9] ibid Rule 30.

permitting a forceful response in self-defense, assuming attribution of the attacker.[10] 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.[11] Apart from this relatively small subset of cyber-intrusions, however, the legal regime remains clouded and ambiguous.

International law scholars and operational lawyers have struggled over the last decade to accommodate LOAC and the UN Charter system to asymmetric warfare waged by non-State actors, including terrorist groups. A similar effort is now underway – evidenced by the *Tallinn Manual* project –to incorporate cyber war in our longstanding positive law systems for protecting civilians from the ravages of war. Yet the language and structure of LOAC – 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. Because cyber-attacks 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. Nor are the Charter threshold requirements – that there be suffered by a victim State a 'use of force' or 'armed attack' before forceful defenses are employed – easily interpreted to accommodate cyber-attacks. Over time, the ongoing struggle to fit cyber into the LOAC and Charter categories may threaten their normative integrity and their basic commitment to collective security and restraints on unilateral uses of force.

Most cyber-intrusions now and in the foreseeable future will take place outside the traditional consensus normative framework for uses of force supplied by international law. For the myriad, multi-layered 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 parts of the chapter summarize the historical and contemporary normative justifications for cyber war. A concluding section emphasizes the importance of coming to some agreement on the central norms for cyber war.

---

[10] ibid Rule 13.
[11] ibid Rules 11, 12.

1. FINDING *AD BELLUM* JUSTIFICATION FOR CYBER WAR

Assume that the fictional State of Evil launches a massive malware attack at the fictional State of Bliss. 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. Evil 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 Evil and Bliss, and pending Security Council action, Bliss is lawfully permitted by Article 51 of the Charter to use self-defense to respond to the 'armed attack' by Evil. The Charter and LOAC norms provide sufficient *ad bellum* authority for Bliss to respond to these cyber-attacks.

Assume instead that a terrorist group has launched a series of cyber-attacks on the banking system of a G-8 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 to the terrorist group, but 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. Surely the G-8 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. Under these circumstances, what *ad bellum* principles should determine the victim State's response?

Although these two simplistic scenarios do not fairly 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 Charter and LOAC framework for cyber-war.

Why is fitting cyber within the traditional framework for armed conflict so difficult? What international law principles offer the best options for extending their application to cyber-attacks? Reforming the international law of cyber is even more difficult because states have different political interests, vulnerabilities and domestic governance and process dynamics.

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'.[12] 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. 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.[13] 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 Charter and LOAC-based *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 traditional approach to assessing *ad bellum* authority to respond to aggression involves assessing the consequences of the attack. What international law determines the permissible responses to a cyber-attack that causes considerable 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

---

[12] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press 2011) 32.

[13] Seymour E. Goodman and Herbert S. Lin (eds), *Toward a Safer and More Secure Cyberspace* (The National Academies Press 2007); William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press 2009).

by an injured State in response to another State's internationally unlawful conduct.[14] In the cyber context, 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 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 *State* to cease its violation.[15]

In the cyber arena, one important question is whether countermeasures include so-called 'active defenses', which attempt through an in-kind response to disable the source of an attack while it is underway.[16] 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.[17] Computer programs that relay destructive viruses to the original intruder's computer or packet-flood the computer have been publicly discussed.[18] 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'.[19]

In theory, countermeasures provide a potentially effective defensive counter to 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

---

[14] ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' [2001] UN Doc A/56/20.

[15] ibid art 49.

[16] Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stanford Journal of International Law 207, 230.

[17] ibid 231.

[18] ibid 231.

[19] US Department of Defense, 'Strategy for Operating in Cyberspace' (2011) 7, 230.

the State responsible, and follow various procedural requirements, delaying execution of the active defense.[20] The delay may be exacerbated by the problems in determining attribution. Second, note that 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,[21] or possibly when the State merely knowingly lets its territory be used for unlawful acts.[22] 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 terrorist groups that act independent 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 a terrorist group unaffiliated with any State, and such groups are less likely to be incentivized by the countermeasures to stop their attacks.

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.[23] Note the potential for tautology in this legal analysis – 'force' in the form of active defense is allowed in response because the responder labels the incoming intrusion a 'use of force'. Taken together, the promise of countermeasures in responding to cyber-attacks is significantly compromised by problems of attribution, timing, efficacy and logic. At the same time, if active defense countermeasures are not considered as 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

---

[20] ILC (n 14) arts 49–52.

[21] ibid art 16.

[22] *UK v Albania* [1949] (ICJ Rep 4); 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 Military Law Review 1.

[23] Jensen (n 16) 231.

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'.[24] In other words, customary law on cyber countermeasures is in flux.

After providing in Article 2(4) that all Member States 'shall refrain … from the threat or use of force against the territorial integrity or political independence of any State',[25] Article 51 creates an exception to the strict prohibition by stating that '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations'.[26] The 'use of force' rubric from Article 2(4) establishes the standard for determining a violation of international law. Once a use of force occurs, permissible responses are determined by the law of State responsibility,[27] potential Security Council resolutions and the law of self-defense. 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,[28] and only to interventions that produce physical damage. As such, most cyber-attacks will not violate Article 2(4).[29] 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.[30] 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.[31]

Article 2(4) is textually capable of evolving to include cyber intrusions, depending on the severity of their impact. Cyber-attacks can cause harm

---

[24] International Group of Experts (n 5) Rule 9.

[25] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(4).

[26] ibid art 51.

[27] Michael N. Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 Villanova Law Review 569, 573–80.

[28] Owens, Dam and Lin (n 13) 253.

[29] Jason Barkham, 'Information Warfare and International Law on the "Use of Force"' (2001) 34 NYU Journal of International Law and Politics 56, 56.

[30] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 421, 421.

[31] ibid 431.

equivalent to kinetic attacks. The imprecision of the text and the growing cyber threat suggests that State practice may now or will in the future recognize cyber intrusions as 'uses of force', at least when cyber-attacks deliver consequences that resemble those of conventional armed attacks.[32] Public statements by the United States in recent years suggest that our 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 our government's history of resisting flexible standards for interpreting Article 2(4).[33] 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.[34] In other words, unilateral responses to a use of force are permitted only if the intrusion constitutes an armed attack recognized by Article 51.

To the extent that cyber intrusions do not meet the criteria for 'use of force', Russell Buchan argues that cyber-attacks that do not cause physical damage violate international law on the basis of the principle of non-intervention as embodied in customary law.[35] Buchan maintains that non-intervention proscribes cyber-attacks that are not destructive so long as the attack is intended to coerce a victim State into a change in policy 'in relation to a matter that the victim State is freely entitled to determine

---

[32] Owens, Dam and Lin (n 13); Waxman (n 30); Abraham D. Sofaer, David Clark and Whitfield Diffie, 'Cyber Security and International Agreements' *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (2010); Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law 885; Oona A. Hathaway, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817; The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011), accessed 19 September 2016 at https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; International Group of Experts (n 5) Rule 11.

[33] Waxman (n 30); Ellen Nakashima, 'Cyberattacks Could Trigger Self-Defense Rule, U.S. Official Says' *The Washington Post* (18 September 2012), accessed 19 September 2016 at https://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html.

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

[35] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 211, 214.

itself'.[36] Although the non-intervention norm has the potential to serve as a legal barrier to disruptive cyber intrusions, there is no indication that any State has relied on Buchan's argument, nor that any court has credited it in a cyber context.

Some scholars have argued that cyber-attacks that are especially destructive but have not been traditionally considered as armed attacks under Article 51 might give rise to the Article 51 right of self-defense.[37] 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 attack on Iranian oil platforms was justified by the right of self-defense following low-level Iranian attacks on U.S. vessels in the Persian Gulf.[38] 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,[39] 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 any case, 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.[40] 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 U.S. 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'.[41] Only if the State admits its collaboration with terrorists[42] or is otherwise found responsible for the terrorists' actions may the victim State use force against the terrorists and sponsoring State.

In recent years, the law of self-defense has been at the center of international law attention. Yet for better or worse, the legal doctrine remains unsettled. The text of Article 51 – 'armed attack' – is not as

---

36 ibid 224.
37 Schmitt (n 32) 930–4; Jensen (n 16) 223–39; Experts (n 5) Rule 13.
38 *Iran v US* [2003] ICJ Rep 161 para 12.
39 ibid.
40 ILC (n 14) art 8.
41 *Nicaragua v US* [1986] ICJ Rep 14; *Prosecutor v Tadic* [1999] Appeals Chamber Judgment.
42 ILC (n 14) art 11.

amenable as 'use of force' to a flexible interpretation (the phrase 'armed attack' is relatively precise). Nor did the Charter drafters consider the possibility that very harmful consequences could follow from a non-kinetic cyber-attack. 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.[43] 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.[44] NATO adopted a similarly worded resolution.[45] 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.[46]

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.[47] While the ICJ has not ratified the

---

[43] Department of Defense Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (1999) 16; Michael N. Schmitt, 'Responding to Transnational Terrorism under the Jus Ad Bellum: A Normative Framework' (2008) 56 Naval Law Review 1; Michael N. Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (2010); Sean Watts, 'Low-Intensity Computer Network Attack and Self-Defense' (2011) 87 International Law Studies 60; Steven R. Ratner, 'Self-Defense Against Terrorists: The Meaning of Armed Attack' in Nico Schrijver and Larissa van den Herik (eds), *The Leiden Policy Recommendations on Counter-Terrorism and International Law* (2012); International Group of Experts (n 5) Rule 13.

[44] 'Security Council Resolution 1368 [2001] UN Doc S/RES/1368.

[45] North Atlantic Treaty Organization, 'Statement by the North Atlantic Council' (2001), accessed 19 September 2016 at http://www.nato.int/docu/pr/2001/p01-124e.htm.

[46] Derek Jinks, 'State Responsibility for the Act of Private Armed Groups' (2003) 4 The Chicago Journal of International Law 83, 89.

[47] Ratner (n 43).

evolving State practice, and even seemed to repudiate it in at least three decisions – twice since 9/11[48] – 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.[49] 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 United States Department of Defense supports the same position.[50] 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.[51]

The legal bases for self-defense have similarly been 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',[52] 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.[53] Imminence in contemporary contexts is measured by reference to a point in time where the State must act defensively before it becomes too late.[54] 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.[55]

---

[48] *Nicaragua v US* (n 40); Wall Street Advisory Opinion [2004] ICJ Rep 136 para 139; *Democratic Republic of the Congo v Uganda* [2005] ICJ Rep 168 para 146.

[49] UN Secretary-General, 'Report of the Secretary-General's Panel of Inquiry on the 31 May 2010 Flotilla Incident' Annex 1; Ratner (n 43) 8–9.

[50] Ratner (n 43).

[51] Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (n 27) 593.

[52] Daniel Webster, in H. Miller (ed), *Treaties and Other International Acts of the United States of America* (1934).

[53] The White House, 'The National Security Strategy of the United States of America' (2010).

[54] Schmitt, 'Responding to Transnational Terrorism under the Jus Ad Bellum: A Normative Framework' (n 43) 18–19; Experts (n 5) Rule 15.

[55] Schmitt, 'Responding to Transnational Terrorism under the Jus Ad Bellum: A Normative Framework' (n 43) 18–19.

In contemporary State practice, nearly every use of force around the world is justified as an exercise of self-defense.[56] 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'.[57] In this environment of expansive interpretations of self-defense relatively unbounded by positive law, the legal parameters of self-defense law as just summarized may be applied to the cyber domain and adapted to cyber-attacks, subject to meeting the Article 51 threshold of armed attack. Applied to non-State actors, 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 unable or unwilling to police its territory. In the sphere of anticipatory self-defense, the fact that cyber-attacks will come unattributed and without warning provide strong analogs to the challenges of counter-terrorism law. At the same time, even though reliance on self-defense arguments is and will remain tempting in the cyber arena, the value of the Charter system in making law for new cyber-response applications is limited by the 'use of force' and 'armed attack' qualifications.

What do the Charter, LOAC and emerging State practice 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.[58] 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 in this section, the international law of self-defense may only justify responses to cyber-attacks that are sufficiently destructive to meet the armed attack threshold, a small subset of cyber intrusions. Still, in limited situations, if a cyber-intrusion is believed to be caused by a non-State terrorist organization (through actual attribution or meeting an imminence requirement in anticipatory self-defense), and the intrusion is sufficiently disruptive as to cause significant harm to important functions in society but does not meet the traditional armed attack criteria, it remains possible that Article 51

---

[56] Watts (n 43).
[57] ibid 76.
[58] International Group of Experts (n 5) Rule 13.

self-defense authority may be extended to permit forceful countermeasures or other forceful responses to a cyber-attack, based on State practice. Whether the development of cyber-law so removed from the text of the Charter represents the optimal path forward for the law of cyber-war will be considered in the final section of this chapter. On the one hand, the Charter's self-defense doctrine as traditionally understood may not leave States adequate authority to respond to the full range of cyber threats they face. On the other hand, the development of customary 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. Of course, even Charter law interpreted at degrees of separation from the Charter is preferable to a legal vacuum.[59] We will see that counterterrorism law may contribute to the development of an international legal paradigm for cyber-defense without producing additional strain on traditional *ad bellum* norms.

2. CONTEMPORARY *AD BELLUM* JUSTIFICATIONS FOR CYBER WAR

For a long time there has been a tendency among some U.S. government officials and legal scholars to denigrate the status of international law generally and/or to claim that international law, whatever its role elsewhere, should not inform law judgments made by U.S. courts or our elected leaders. In the fields of national security and counterterrorism, however, spurred by the often eloquent and remarkably able efforts of State Department legal advisers and others over several recent administrations, we have also learned that international law has in fact played a major role in shaping national security and counterterrorism policies and operations, and that international law has been respected by senior U.S. officials of both parties. Indeed, the domestic politics of legal change have been very much on display in the United States. Largely in response to modern terrorism, actors in the U.S. government have worked to expand conventional understandings of international law principles independent of accepted doctrine and judicial decisions in the area.

[59] Watts (n 43) 66.

Yet the Global War on Terror era in the years immediately after 9/11 and the invasion of Iraq without Security Council authorization in 2003 led many critics to observe that the United States was going its own way legally, at the expense of international law and the harmony of international relations among traditional allies. During the second term of President George W. Bush and throughout the Obama administration considerable effort has been made to articulate the international law bases for U.S. actions in pursuit of national security and counterterrorism objectives abroad, and the relative openness of administration lawyers about the law, including international law, has helped restore some confidence that international law matters in our government's decision-making calculus.

Despite the best efforts of some of the keenest legal minds and most lucid juridical and scholarly formulations, international law generally and LOAC in particular do not supply a clear, complete and coherent *ad bellum* framework for cyber war. The 'use of force' and 'armed attack' thresholds were written to limit kinetic actions. Using persuasive arguments that the measure of invoking these 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 others have shown how cyber-attacks may cause harm that should count as uses of force and, less plausibly, armed attacks. Their view is that once the gateway determinations are made to reach the cyber domain, LOAC supplies at least a serviceable roadmap for limiting cyber-war.

In activating the U.S. Cyber Command in 2010, the Department of Defense confronted Congressional scepticism and challenges from across the political spectrum that focused on 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 nation's largely privately held critical infrastructure.[60] While Congress and other interested constituencies have continued to wrestle with the policy, scope of authorities and privacy questions, from the beginning Cyber Command and the Department of Defense generally have indicated that existing Charter and LOAC-based law adequately support the authorities of the United States to defend the United States from cyber-attack.[61] Indeed, in

[60] Ellen Nakashima, 'Cyber Command Chief Says Military Computer Networks Are Vulnerable' *The Washington Post* (4 June 2010), accessed 19 September 2016 at http://www.washingtonpost.com/wp-dyn/content/article/2010/06/03/AR2010060302355.html.

[61] Watts (n 43).

2013 President Obama issued a classified policy directive that detailed certain criteria and basic principles for U.S. responses to cyber intrusions, including defensive and offensive cyber operations.[62]

As this chapter has shown, however, there is no consensus that the Charter schema supplies a coherent or adequate set of norms for regulating cyber-warfare. Particularly for cyber-attacks that are especially disruptive but not destructive – intrusions that may be increasingly pervasive, operating beneath the radar of existing defensive mechanisms, and capable of fairly easily and cheaply being perpetrated by virtually any State or non-State actor – the Charter provides only the sketchiest of normative blueprints. The recurring theme that the LOAC bifurcate international relations into states of war or peace is prominently displayed in the cyber arena. If the armed attack threshold is met, forceful responses may be employed. Otherwise only 'peaceful' defenses are lawful. The asymmetric opportunities for non-State adversaries abound, and under the Charter norms victim States may have to choose between defending themselves unlawfully and absorbing continuing cyber-attacks.[63]

Starting with the text of the Charter, this chapter has shown that arguments to apply the 'use of force' and 'armed attack' Charter categories to cyber attack 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 similar response may not be considered an armed attack.[64] The fact that it may be possible simply to characterize a new form of intrusion – cyber-attack – as a use of force or armed attack is not wholly 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'[65] approach to deciding when the intrusion constitutes a 'use of force' or 'armed attack' that would trigger LOAC 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.

---

[62] 'Obama Tells Intelligence Chiefs to Draw up Cyber Target List – Full Document Text' *The Guardian* (7 June 2013), accessed 19 September 2016 at http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

[63] ibid 60–61.

[64] Counsel (n 43).

[65] *Jacobellis v Ohio* [1964] 378 US 184, 197.

Relying on self-defense as a legal justification for responding forcefully to cyber-attacks would not constitute the first time that States have argued for Article 51 authority to respond with military force to a provocation that is something other than a traditional 'armed attack'. At least since the 1986 bombing of Libyan command and leadership targets in response to a Berlin disco bombing attributed to Libya the United States has been criticized in the international community for maintaining that it has an inherent right to use force in self-defense against acts that do not constitute a classic armed attack.[66] In addition, under the terms of the Charter, forceful responses against non-State actors are handicapped at the outset because the Charter was drafted to regulate relations among States. Still, for understandable reasons, States tend to defend all their uses of force as self-defense.[67] The reliance by the United States on self-defense in its targeting of terrorists outside traditional battle spaces is emblematic of the tendency to freight legally unsettled and controversial uses of force onto the Charter provision, without Security Council approval or international judicial recognition. Of course the threats to U.S. interests have been real, if unconventional, and the open-textured language of Article 51 is the single alluring source of positive law authority that may support the expansive uses of force.

However sympathetic we may be to the very real threats to national security presented by non-State terrorists wielding unconventional weapons, unannounced, against civilians, the Charter's role in supplying the *jus ad bellum* support for the use of force in defending against a wide range of terrorist attacks including cyber is open to question.[68] As Sean Watts warned, over time the written law of the Charter may take a back seat to the supposed law of self-preservation.[69] At the same time, the Charter's use of force/armed attack paradigm may be construed to support justifications for self-defense actions that do more to harm than protect peace and security. For example, a 1999 Department of Defense Office of General Counsel assessment of information operations maintained that when a cyber-attack is considered equivalent to an 'armed attack', and it is not possible or appropriate to respond by attacking the specific source of the computer attack, 'any legitimate military target could be attacked … so long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to

---

66 Counsel (n 43) 16.
67 Watts (n 43).
68 ibid.
69 ibid.

undertake them'.[70] Although such a response may be lawful under LOAC, the decision to attack 'any legitimate military target' runs the risk of escalation of a non-kinetic information operation to something more lethal.

Meanwhile, it may be that the dynamic growth of reliance on the Internet to support our infrastructure and national defense 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 Waxman has noted, U.S. government statements may be interpreted to suggest that only cyber-attacks that have especially harmful effects will be treated as armed attacks, while lower level intrusions would enable cyber countermeasures in self-defense.[71] If the statements represent U.S. policy, 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.[72] 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 riles international lawyers and injects ever more subjectivity and less predictability into future self-defense projections. Taking into account the characteristics of cyber-war – uncertainty, secrecy and lack of attribution – finding consensus on international regulation through these Charter norms will be a tall order.[73]

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 can support responses that protect national and human security. Anonymity and surprise have long been central tenets of terrorist attacks, and international law has developed normative principles – such as anticipatory self-defense – that accommodate these characteristics. By analogy international law can 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

---

[70] Counsel (n 43).
[71] Waxman (n 30) 439.
[72] ibid 439.
[73] ibid 443.

learning that an attack comes from within a certain State does not tell us whether the attack is State-sponsored or was done by a non-State actor. Because existing Charter and LOAC 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 no clear LOAC or Charter-based authority to go after the private attackers inside a State when that State was not involved in the attacks.[74] International law offers an alternative normative path, if criteria can be developed that tell decision-makers when 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 analogies to ongoing United States actions in its counterterrorism targeting program are striking.[75]

International law governing cyber-war will emerge unevenly, over time, as the product of State, regional and perhaps even global policies and strategies. 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, LOAC or customary law would stand in its way, except to the extent that espionage involving military weapons systems constitute armed aggression.[76] 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 striking and troubling. It is possible that LOAC could develop customarily to recognize legal limits on cyber-exploitation where the software agent is capable of destructive action or may facilitate the same.[77] As cyber-exploitation assumes an ever more important role in States' cyber-defenses, might the international community consider developing some regulatory principles as part of counterterrorism law?

In the intelligence regulation respect and others international law for cyber-operations may evolve through something like natural law-type or

---

[74] International Group of Experts (n 5) Rule 6.

[75] Robert M. Chesney, 'Who May Be Held? Military Detention Through the Habeas Lens' (2011) 52 Boston College Law Review 769.

[76] Roger D. Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 Air Force Law Review 217, 223–4.

[77] Owens, Dam and Lin (n 13) 261, 263.

just war theory reasoning, as has been the case with development of some other international law norms.[78] 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.[79] Ironically, as some prominent U.S. academics developed theories of 'vertical domestication'[80] to encourage greater respect and adherence to international law by the U.S. government, in the last decade the U.S. 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 U.S. government policies and practices, counterterrorism law has matured and developed normative content around some of its revised tenets, such as military detention and the use of military commissions.[81] States may develop legal authorities in this emerging paradigm of cyber-war through a similar process.

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 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.[82]

---

[78] Jeffrey L. Dunoff and Mark A. Pollack, 'What Can International Relations Learn From International Law?' (2012) 11 Temple University Legal Studies.

[79] W. Michael Reisman, 'Assessing Claims to Revise the Laws of War' (2003) 97 American Journal of International Law 82.

[80] Harold H. Koh, 'Transnational Legal Process' (1996) 75 Nebraska Law Review 181; Harold H. Koh, 'The 1998 Frankel Lecture: Bringing International Law Home' (1998) 35 Houston Law Review 623, 626–7.

[81] Chesney (n 75).

[82] Owens, Dam and Lin (n 13) 245.

For the United States, the fact that so much of our infrastructure is privately owned makes securing the infrastructure legally and practically problematic,[83] and yet our heavy reliance on networked information technology makes us highly vulnerable to cyber-intrusions. Our 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'[84] 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.[85] 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.

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 LOAC-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.[86] As this part has shown, law follows political contestation, too. In the cyber realm, the disparate political interests and governmental processes of the nation states with a great deal at stake in cyber have made norm development particularly challenging.

---

[83] Waxman (n 30) 451.
[84] ibid 452.
[85] ibid 453.
[86] ibid 455–7.

3. CONCLUSIONS

Imagine one more scenario. This one takes place during 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 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.[87] 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 captives contained similar details about U.S. 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 mentioned above. The governments of Russia, China and Iran have denied any involvement in the attacks, and no intelligence points to their involvement. Al-Qaeda has shown interest in cyber-war capabilities, and the seized laptops suggest that some steps were taken to acquire them.

Assuming that the United States concludes that Al-Qaeda is most likely behind the attacks, what law governs the response? If, instead, we decide that the attacks were launched by Russian intelligence operatives

[87] Brenner (n 12) 96–7.

situated in South Asia, what law governs the response? This chapter has helped draw attention to the incompleteness of the legal regime that will be required to provide the normative justifications for responding to these intrusions.

The stakes are escalating. The United States used offensive cyber weapons with Stuxnet to target Iran's nuclear program, and nation States and non-State actors are aware that cyber warfare – offensive and defensive – has arrived with 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 U.S./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 offensive cyber-attacks,[88] Stuxnet created the precedent, as did Israel's cyber-attack on Syrian air defenses when it attacked a suspected Syrian nuclear site in 2007,[89] Russia's cyber-attacks in its dispute with Georgia,[90] and the apparent use of cyberweapons by the United States to target Al-Qaeda websites and terrorists' cell phones.[91] Now that the cyber war battlefield apparently has expanded to Beirut banks and a neutral State,[92] 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 war will be especially difficult, particularly determining what kinds of cyber-attacks trigger the authority to take defensive actions and the nature of the defenses that will be permitted. 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

---

[88] Eric Schmitt and Thom Shanker, 'U.S. Debated Cyberwarfare in Attack Plan on Libya' *The New York Times* (17 October 2011), accessed 19 September 2016 at http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

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

[90] John Markoff, 'Before the Gunfire, Cyberattacks' *The New York Times* (12 August 2008), accessed 19 September 2016 at http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[91] ibid; Jack Goldsmith, *Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya* (Lawfare 2011).

[92] Katherine Maher, 'Did the Bounds of Cyber War Just Expand to Banks and Neutral States?' *The Atlantic* (17 August 2012), accessed 19 September 2016 at http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/.

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.[93] 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 in general and the United States in particular run some significant risks by continuing to build cyber-war law using the Charter/LOAC 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.[94] If, over time, the thresholds for what constitutes an armed attack are lowered to reach more forms of cyber-attack, legal barriers to military force will be lowered at the same time, leading to more military conflicts in more places. The high threshold for invoking the Charter's self-defense authorities traditionally supported by 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.[95]

Yet the high self-defense threshold also leaves unregulated (at least by the Charter and LOAC) 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.[96] If States or the international community attempt to further expand the reach of self-defense and LOAC in idiosyncratic ways to non-destructive cyber intrusions, the Charter and LOAC will be compromised.

The effects-based approach to interpreting the Charter and LOAC in the cyber realm tends toward incoherence and lacks a normative core. Customary international law could support or help build the normative architecture for cyber-operations, at least at the margins, where the legal landscape is not now clear. Over time a cyber-regime may develop that

---

[93] Waxman (n 30) 448.

[94] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation 2009); O'Connell (n 2).

[95] Waxman (n 30) 446–7.

[96] International Group of Experts (n 5) Rule 9.

supplements the Charter and LOAC and permits forceful responses to especially destructive intrusions while preserving some yet-to-be-defined lower-intensity options for less harmful attacks.

More particularly, 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 and have been 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.

The Charter and LOAC-based cyber-law that has developed in fits and starts over recent decades is reminiscent of the adage that if you only have a hammer, you see every problem as a nail. We have invested in military capabilities for cyber, so it has become a military use of force legal problem. Cyber is not fundamentally a problem for the military, and the Charter and LOAC do not provide all the answers.