INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare

William Banks

89 INT'L L. STUD. 157 (2013)

Volume 89 2013

The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare

William Banks[*]

I. INTRODUCTION

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 are forced to shut down, incoming payments due from abroad cannot arrive and government ministries close up shop. Credit card companies shut down their networks worldwide, fearing the

[*] Board of Advisors Distinguished Professor of Law; Director, Institute for National Security and Counterterrorism; Professor of Public Administration and International Affairs, Syracuse University. The author is grateful to Eric Jensen and Matthew Waxman for helpful comments on a draft version, and to Erin Lafayette and Egon Donnarumma for excellent research assistance.

spread of the attacks. Meanwhile, the national government closes 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 are high and mounting.

As the government's security, intelligence and law enforcement resources scramble to identify the source of the attacks and implement defensive measures, legal advisers face their own challenges. The first intelligence reports show 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 unidentified 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?

The prospect of cyber war has evolved from science fiction and over-the-top doomsday depictions on television, films and in 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 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.[1] 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

1. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all; *see also* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

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?

Most computer attacks temporarily disable the computer or its applications, or exploit the computer by reporting back data to a remote host. More sophisticated intrusions, however, can cause more significant disruptions or even destruction, like the Iranian centrifuges or worse. Because our societies now entrust so much of our critical infrastructure to online systems, experts such as former Clinton and Bush administration cyber and counterterrorism adviser Richard A. Clarke warn that cyber attackers could derail trains, cause power blackouts, cause oil or gas pipelines to explode, or ground aircraft.[2]

Whether large or small, cyber attacks are proliferating, at least in part because the means are becoming cheaper and easier to acquire and use.[3] Particularly when targeted at powerful adversaries like the United States, cyber intrusions offer a model application of asymmetric warfare, where adversaries much weaker in conventional terms exploit vulnerabilities in the stronger foe. The asymmetric attackers are further advantaged by the fact that they may mask their identity and location at least temporarily and avoid immediate attribution and response to the attacks. As such, cyber attacks share core characteristics with other terrorist attack modes. As the means to affect cyber attacks become easier to acquire and use, terrorists may wage cyber war against their adversaries, either directly attacking government systems or going after infrastructure in the private sector.

Relatively little has been written about the legal bases for countering cyber terrorism,[4] and it has yet to be considered whether counterterrorism law could illuminate *ad bellum* norms for responding to cyber attacks perpetrated by terrorists or where the source of an attack cannot be promptly attributed and terrorists are suspected. The relative lack of attention given by States and international law experts to counterterrorism law as a source of authority to govern responses to cyber attacks is not surprising in view

2. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 64–68 (2010).

3. *See id.*; JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 154 (2011).

4. Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 JOURNAL OF INTERNATIONAL BUSINESS AND LAW 1 (2010); Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY 437, 448–49 (Franklin D. Kramer et al. eds., 2009).

of the difficulties more generally in the international community to identify and agree upon a legal paradigm for counterterrorism.[5] Although the international community continues to struggle to find an acceptable definition of terrorism,[6] it is generally understood that a cyber terrorist "uses Internet-based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks."[7] Like terrorism generally, cyber terrorism intends "to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. . . . Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples."[8]

Meanwhile, the prospects for the use of cyber weapons by and against terrorist groups are increasing. Research conducted in the period immediately after the 9/11 attacks suggested that, although terrorists' interest in cyber attacks was increasing, their capabilities then were demonstrated only for theft and low-level attacks.[9] By implication, more disruptive or damaging versions of cyber terrorism could become a significant threat in the future. Meanwhile, at least since 2008 reports document likely Western government uses of cyber weapons against terrorist websites,[10] and U.S. use of cyber intrusions aimed at cell phone communications among terrorist leaders that could lure them to an ambush, spread false information that fellow jihadists were conspiring against their comrades and otherwise incite distrust of their supposedly secure communications.[11]

Even as experts recognize that terrorists may engage in cyber war, the international community continues to rely on a legal conception that limits

---

5. *See, e.g.*, Rosalyn Higgins, *The General International Law of Terrorism*, *in* TERRORISM AND INTERNATIONAL LAW 13, 13–14 (Rosalyn Higgins & Maurice Flory eds., 1997) ("terrorism is not a discrete topic of international law with its own substantive legal norms"); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 745 (7th ed. 2008) ("There is no category of the 'law of terrorism' and the problems must be characterized in accordance with the applicable sectors of public international law . . . .").

6. STEPHEN DYCUS ET AL., COUNTERTERRORISM LAW 5–6 (2d ed. 2012).

7. SANDIA NATIONAL LABS., CYBER THREAT METRICS 11 n.4 (Sandia Report SAND2012-2427, Mar. 2012), *available at* http://prod.sandia.gov/techlib/access-control.cgi/2012/122427.pdf.

8. Dorothy E. Denning, *Is Cyber Terrorism Next?, in* UNDERSTANDING SEPTEMBER 11, at 193 (Craig Calhoun, Paul Price & Ashley Timmer eds., 2002).

9. *Id.* at 135–36; *see also* Lachow, *supra* note 4.

10. *See, e.g.*, Ian Black, *Cyber-attack theory as al-Qaida websites close*, GUARDIAN, Oct. 22, 2008, International Pages, at 16.

11. Eric Schmitt & Thom Shanker, *After 9/11, an Era of Tinker, Tailor, Jihadist, Spy*, NEW YORK TIMES, Aug. 7, 2011, § SR, at 6.

terrorism to "acts of violence committed in time of peace,"[12] a categorization that excludes most, though not all, cyber attacks. 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.[13] The resulting *Tallinn Manual on the International Law Applicable to Cyber Warfare* 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."[14] The *Tallinn Manual* experts concluded that cyber attacks can constitute terrorism, but only where the attack has been conducted through "acts of violence."[15] 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 of "use of force" or "armed attack."[16] 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.[17] To date there has been little attention given to the possibility that international law generally and counterterrorism law in particular could and should develop a subset of cyber-counterterrorism law to respond to the inevitability of cyber attacks by terrorists and the use of cyber weapons by governments against terrorists, and to 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

12. Jelena Pejic, *Armed Conflict and Terrorism: There Is a (Big) Difference*, *in* COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE 203 (Ana Maria Salinas de Frías, Katja L.H. Samuel & Nigel D. White eds., 2012).

13. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

14. *Id.*, rule 36.

15. *Id.*, rule 36, cmt. 2; rule 30.

16. *Id.* at 18.

17. *Id.*, rule 30, cmt. 12 (the majority of the International Group of Experts concluded that cyber intrusions that cause large-scale adverse consequences throughout the State but no physical damage do not trigger LOAC rules).

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 battlespace 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 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–September 11 customary law permitting a forceful response in self-defense, assuming attribution of the attacker.[18] 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.[19] 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 under way—evidenced by the *Tallinn Manual* project—to incorporate cyber war in our long-standing 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

18. *Id.*, rule 13.

19. TALLINN MANUAL, rule 11–12.

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, multilayered and multifaceted 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. In this article, my interest is directed at a subset of those cyber attacks—those where terrorists are responsible or attribution is not known but points in the terrorists' direction, and where the effects are very disruptive but not sufficiently destructive to cross the traditional LOAC and Charter self-defense thresholds.

For this subset of cyber attacks, counterterrorism law may offer a useful complementary normative supplement to LOAC and the Charter. Especially over the last decade, a corpus of counterterrorism law has evolved as domestic and international law in response to transnational terrorism. In contrast to the dominant pre–September 11 conception that countering terrorism involved either the use of military force or enforcement of the criminal laws, counterterrorism law now incorporates a diverse range of responses to terrorism, many of which are borrowed, sometimes in modified form, from existing international and domestic law. Based on a maturing international legal regime, this article concludes that over time and through State practice, along with legal, strategy and policy development in the international community, a set of counterterrorism law norms for cyber war could emerge.

In this article, I will first review the *ad bellum* justifications for conducting cyber war within the Charter and LOAC systems. The international law doctrines permitting countermeasures offer one set of options, and the possibility that cyber intrusions could constitute an unlawful intervention, "use of force" or "armed attack" will also be considered briefly. I 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.[20] Part III traces the sources and contents of counterterrorism law that could provide the normative bases for cyber war in some circumstances. In light of the analysis in Parts II and III, Part IV will speculate concerning how an international counterterrorism law might develop in the cyber domain. As has been the case with counterterrorism law generally, a cyber-oriented counterterrorism law will follow the eventual development and implementation of national and international policies and strategies to counter cyber threats.

II. 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 IAC, either because there is no known State adversary either because there has been no "attack" as contemplated by Article 49 of the Third Geneva

20. *See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 187, 190–91, 199 (2012).

Convention. 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?

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."[21] 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.[22] 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 respond-

21. BRENNER, *supra* note 3, at 32.

22. *See* NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE (Seymour E. Goodman & Herbert S. Lin eds., 2007); NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES § 2.4.2 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter TECHNOLOGY, POLICY, LAW, AND ETHICS].

ing 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—lawful actions undertaken by an injured State in response to another State's internationally unlawful conduct.[23] 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 International Law Commission's Draft Articles on Responsibility of States 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.[24]

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 under way.[25] Whatever active defense technique is 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.[26] Computer programs that relay destructive vi-

---

23. U.N. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ch. II, U.N. GAOR, 53d Sess. Supp. No. 10, at 80, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter *Draft Articles on Responsibility of States for Internationally Wrongful Acts*].

24. *Id.*, art. 49 (emphasis added).

25. *See* Eric T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STANFORD JOURNAL OF INTERNATIONAL LAW 207, 230 (2002).

26. *Id.* at 231.

ruses to the original intruder's computer or packet-flood the computer have been publicly discussed.[27] 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."[28]

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 the State responsible and follow various procedural requirements,[29] delaying execution of the active defense. 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,[30] or possibly when the State merely knowingly lets its territory be used for unlawful acts.[31] 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

27. *Id.*

28. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; *see also* Jensen, *supra* note 25, at 230.

29. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, arts. 49–52.

30. *Id.*, art. 16.

31. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9). *See also* 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*, 201 MILITARY LAW REVIEW 1, 43 (2009).

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.[32] 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 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 has ended."[33] 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,"[34]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."[35] 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,[36] 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

32. Jensen, *supra* note 25, at 231.

33. TALLINN MANUAL, *supra* note 13, rule 9, cmt. 3.

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

35. *Id.*, art. 51.

36. *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA LAW REVIEW 569, 573–80 (2011).

of self-defense apply to armed violence, such as military attacks,[37] and only to interventions that produce physical damage. As such, most cyber attacks will not violate Article 2(4).[38] 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.[39] 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.[40]

Article 2(4) is textually capable of evolving to include cyber intrusions, depending on the severity of their impact. Cyber attacks can cause harm 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.[41] 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).[42] As historically interpreted, however, the Charter

37. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 253.

38. *See* Jason Barkham, *Information Warfare and International Law on the "Use of Force,"* 34 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 56 (2001).

39. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 428 n.32, 429–30 nn.37–38 (2011).

40. *Id.* at 431.

41. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 33-34; Waxman, *supra* note 39, at 432 n.48 (citing Abraham D. Sofaer et al., *Cyber Security and International Agreements, in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 185 (2010)). *See also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999) (proposing that cyber attacks could constitute use of force if they meet several practical measures of harm). *See also* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 848 (2012); THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 14 (2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]; *see also* TALLINN MANUAL, *supra* note 13, rule 11.

42. Waxman, *supra* note 39, at 436–37. *See* Ellen Nakashima, *U.S. official says cyberattacks can trigger self-defense rule*, WASHINGTON POST (Sept. 18, 2012), http://articles.washing

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 unless it is a lawful action in self-defense.[43] 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.[44] 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 itself."[45] 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, or that any court has credited it in a cyber context.

Some scholars have argued that cyber attacks that are especially destructive but have not traditionally been considered armed attacks under Article 51 might nonetheless give rise to the Article 51 right of self-defense.[46] But no international tribunal has so held. In a case involving conventional armed violence, but on a small scale, the United States argued unsuccessfully before the International Court of Justice (ICJ) that its naval attacks on Iranian oil platforms were justified by the right of self-defense following low-level Iranian attacks on U.S. vessels in the Persian Gulf.[47] Although the separate opinion of Judge Simma in the *Oil Platforms* case ar-

---

tonpost.com/2012-09-18/world/35497194_1_international-law-legal-adviser-cyberspace (noting that State Department Legal Adviser Harold Koh stated that any use of force triggers the right of self-defense, and cyber attacks that result in injury, death, or significant destruction would be seen as a violation of international law).

43. *See* Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL LAW REVIEW 132, 172–74 (2005) (concluding that the "use of force" and "armed attack" formulations do not apply to all but a few of the most extreme cyber incidents).

44. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 211, 214 (2012).

45. *Id.* at 224.

46. Jensen, *supra* note 25, at 223–39; Schmitt, *supra* note 41, at 930–34; *see also* TALLINN MANUAL, *supra* note 13, rule 13, cmt. 9.

47. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 46–47 (Nov. 6).

gued that self-defense should permit more forceful countermeasures where the "armed attack" threshold has not been met,[48] 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.[49] 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."[50] Only if the State admits its collaboration with terrorists[51] 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 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.[52] The text of Article 51 does not limit armed

48. *Id.*, ¶ 12 (opinion of Simma, J.).

49. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, art. 8.

50. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 115, 109 (June 27). A somewhat different approach was taken by the International Criminal Tribunal for the former Yugoslavia in *Tadić*, where the Court focused on whether the Federal Republic of Yugoslavia exercised "overall control" of the Bosnian Serb armed groups. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 145 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999).

51. *See Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, art. 11.

52. Steven R. Ratner, *Self-Defense Against Terrorists: The Meaning of Armed Attack, in* LEIDEN POLICY RECOMMENDATIONS ON COUNTER-TERRORISM AND INTERNATIONAL LAW (Nico Schrijver & Larissa van den Herik eds., forthcoming 2012); Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework*, 56 NA-

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.[53] NATO adopted a similarly worded resolution.[54] 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.[55]

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.[56] 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[57]—the trend is to accept the extension of armed attack self-

---

VAL LAW REVIEW 1, 7–13 (2008). 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, *supra* note 41, 151, 163–64; Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense,* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 59, 75–76 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); Office of General Counsel, U.S. Department of Defense, An Assessment of International Legal Issues in Information Operations 16 (May 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter An Assessment of International Legal Issues]; *see also* TALLINN MANUAL, *supra* note 13, rule 13, cmt. 16 (majority of the Group of Experts agree that a cyber attack by terrorists may constitute an armed attack).

53. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

54. Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm.

55. *See* Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHICAGO JOURNAL OF INTERNATIONAL LAW 83, 89 (2003).

56. Ratner, *supra* note 52, nn.5–6.

57. In the *Nicaragua* case, the ICJ never considered whether paramilitary activity by the contras or the FMLN was an armed attack, and focused only on whether their activities could be imputed to the States involved. In *Armed Activities on the Territory of the Congo*, the Court stated that attacks by armed groups could not trigger Article 51, because they

defense authorities when non-State groups are responsible, provided the armed attack predicate is met and the group is organized and not a set of isolated individuals.[58] Unsurprisingly, the U.S. Department of Defense supports the same position.[59] 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.[60]

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-defence is instant, overwhelming, and leaving . . . no moment for deliberation,"[61] 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.[62] Imminence in contemporary contexts is measured by reference to a point in time where the State must act defensively before it becomes too late.[63] In addition to imminence or immediacy, the use of force in self-defense must be necessary—law enforcement or

---

were "non-attributable to the DRC," though at another point the Court stated that it would not address whether self-defense applies against "large-scale attacks by irregular forces." Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶¶ 146–47 (Dec. 19). In the *Wall* opinion, the Court maintained that self-defense is available in State-on-State conflicts, and found self-defense inapplicable partly because Israel did not allege that the harmful acts were imputable to a foreign State. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, § 139 (July 9).

58. *See, e.g.,* U.N. Secretary-General, *Report of the Secretary-General's Panel of Inquiry on the 31 May 2010 Flotilla Incident*, Annex 1, § 41, at 93 (Sept. 2011); Ratner, *supra* note 52, at 8–9.

59. Ratner, *supra* note 52, n.32

60. Schmitt, *supra* note 36, at 593.

61. Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, British Special Minister (Aug. 6, 1842), *reprinted in* 2 JOHN MOORE DIGEST OF INTERNATIONAL LAW 411–12 (1906).

62. *See, e.g.*, THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 22 (2010).

63. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 16–19; *see also* TALLINN MANUAL, *supra* note 13, rule 15 (describing variations on an imminence requirement).

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.[64]

In contemporary State practice, nearly every use of force around the world is justified as an exercise of self-defense.[65] 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."[66] 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* the latter 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 provides strong analogs to the challenges of counterterrorism 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.[67] 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 immi-

64. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 18–19.

65. Watts, *supra* note 52, at 87 n.142.

66. *Id.* at 76.

67. TALLINN MANUAL, *supra* note 13, rule 13, cmt. 8.

nence 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 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 article. 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. Even Charter law interpreted at degrees of separation from the Charter is preferable to a legal vacuum.[68] 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.

III. THE POTENTIAL FOR APPLICATION OF COUNTERTERRORISM LAW

Counterterrorism law is immature, in flux and heavily contested. This section will show that, despite resistance from many quarters and a two-steps-forward-one-step-back development in the United States, counterterrorism law deserves recognition as a discrete and integral part of international law. As the international community gradually embraced the idea that violent terrorism by non-State actors justifies the use of force pursuant to the *jus ad bellum*, several treaties and agreements, Security Council resolutions, and State practice are beginning to recognize counterterrorism law as a sort of hybrid blend of several components of international law. The cyber domain is not yet part of the new corpus, but its time may have arrived.

As Adam Roberts noted more than ten years ago, counterterrorism operations are not entirely like or unlike armed conflicts or other wars.[69] The fact that counterterrorism involves the use of military force along with pursuit of law enforcement and other non–use of force methods involves awkward confluences with international law generally and with *ad bellum*

68. *See* Watts, *supra* note 52, at 66.

69. Adam Roberts, *The Laws of War in the War on Terror*, *in* INTERNATIONAL LAW AND THE WAR ON TERROR 175, 227–28 (Fred L. Borch & Paul S. Wilson eds., 2003) (Vol. 79, U.S. Naval War College International Law Studies).

and *in bello* principles in particular. By and large, the awkwardness has been explained away by international law scholars in the past in their assertions that there simply is no international law concerning terrorism.[70] Undeniably, however, there is now an evolving international counterterrorism law. Through thirteen international treaties, several Security Council resolutions, State practice and emerging policies counterterrorism is developing as an international law paradigm in ways similar to human rights law development in earlier years.[71] The counterterrorism methods are not new, for the most part, and the counterterrorism paradigm does not so much reject the LOAC/armed conflict/war models as offer a complement to them.

That the field of international counterterrorism law is gaining recognition among practitioners and scholars is reflected by the publication of two comprehensive treatises covering counterterrorism law in recent years, each with a stable of distinguished jurists, lawyers and scholars as contributors, and both intent on surveying the state of law in a growing and complex field.[72] Selections from their combined tables of contents are illustrative: counterterrorism and the rule of law framework, multidisciplinary perspectives, UN counterterrorism instruments, judicial and non-judicial responses to terrorism, criminal laws and jurisdiction, investigations and prosecutions, pretrial and trial issues, combating terrorism financing, alternative remittance systems, human rights in countering terrorism and international cooperation.[73] As explained by Katja Samuel in the 2012 volume of *Counter-Terrorism: International Law and Practice*, the "backbone of the existing international [counterterrorism] rule of law framework" consists of human rights law, humanitarian law, criminal law and refugee/immigration law, along with the Charter and general international law principles.[74]

Just as it is noteworthy that international counterterrorism law has emerged as a discrete field, the omission of any treatment of international cyber law in the treatises is striking. In the cyber realm, instead of treating

---

70. *See, e.g.*, Higgins, *supra* note 5; BROWNLIE, *supra* note 5.

71. *See* Daniel Moeckli, *The Emergence of Terrorism as a Distinct Category of International Law*, 44 TEXAS INTERNATIONAL LAW JOURNAL 157, 167–68 (2008). *See also* Cohen, *supra* note 4.

72. AVINDER SAMBEI ET AL., COUNTER-TERRORISM LAW AND PRACTICE (2009); COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12.

73. SAMBEI ET AL., *supra* note 72; COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12.

74. Katja L.H. Samuel, *The Rule of Law Framework and its Lacunae: Normative, Interpretive, and/or Policy Created?*, *in* COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12, at 14.

cyber attacks by terrorists in the either/or dichotomy as crimes or equivalent to kinetic attacks, counterterrorism law may prescribe a range of responses, including intelligence collection and threat identification, border controls, asylum and refugee status rules and procedures, controls on providing financial support to terrorists and kinetic options, the contents of which may vary from traditional LOAC use of force, depending on the harm caused by the attacks. Particularly over the decade after 9/11, counterterrorism matured as a legal regime composed of primary rules, including Security Council resolutions requiring that States take steps to counter terrorism and various treaties, and secondary rules that monitor enforcement of the counterterrorism tools and add norms to counterterrorism in subsidiary areas, such as international criminal law and armed conflict.[75] Unsurprisingly, the development of an international law of counterterrorism reflects parallel developments at the national level in many States.[76]

Counterterrorism law is similarly evolving as domestic law in the United States. Before the 9/11 attacks, the U.S. Army defined counterterrorism as "offensive military operations designed to prevent, deter and respond to terrorism."[77] The Defense Department recognized after 9/11 that "some significant policy and strategy adjustments were required"[78] to counterterrorism doctrine owing to the evolution of the terrorist threat and to conform U.S. military doctrine to international law (the pre-9/11 definition may have permitted actions in violation of Article 2(4) of the Charter). The National Security Strategy of the United States also gradually showed a maturing understanding of the role of counterterrorism. The 2002 Strategy became immediately controversial because of its articulation of an apparent doctrine of preemption.[79] By 2006, the preemption language was moved from the section on terrorism to a section focusing on weapons of mass destruction, and the Strategy recognized that the counterterrorism paradigm involves more than criminal law enforcement and reorientation of the

---

75. Moeckli, *supra* note 71, at 167–68. *See also* Gregory E. Maggs, *Assessing the Legality of Counterterrorism Measures without Characterizing Them as Law Enforcement or Military Action*, 80 TEMPLE LAW REVIEW 661 (2007).

76. *See generally* GLOBAL ANTI-TERRORISM LAW AND POLICY (Victor V. Ramraj et al. eds., 2d ed. 2012).

77. Chairman, Joint Chiefs of Staff, Joint Publication 3-26, Counterterrorism v (2009) [hereinafter Joint Publication 3-26].

78. *Id.*

79. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002).

norms for war.[80] Concerning the use of force in counterterrorism, the measure of imminence in self-defense had evolved in domestic law as it had in international law due to the anonymity and surprise factors in terrorist attacks and was measured as much by the availability of an opportunity to respond as by the immediacy in time of the anticipated attack.[81] Likewise, territorial sovereignty weakened as a barrier to action in self-defense.[82] By 2009, the Department of Defense had broadened considerably its definition of counterterrorism: "actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks."[83] So understood, counterterrorism "is an activity of irregular warfare" and its "efforts should include all instruments of national power to undermine an adversary's power and will, and its credibility and legitimacy to influence the relevant population."[84]

As a baseline proposition, in the twenty-first century there can be little doubt that violent terrorism justifies the use of force in countering terrorist attacks pursuant to the *jus ad bellum*. Any shortcomings in the normative foundation for counterterrorism law were effectively erased after the 9/11 attacks and passage of Security Council Resolutions 1373 and 1377. Even in the years before 9/11, the Security Council recognized that terrorism could constitute a breach of peace and security.[85] Although the Council has not authorized the use of force in response to terrorism, it could do so.[86] The Counterterrorism Committee of the United Nations Security Council was established in 2001 by Resolution 1373, which determined "to combat by all means threats to international peace and security caused by terrorist

80. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 23 (2006).

81. *See* Watts, *supra* note 52.

82. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 27–30.

83. Joint Publication 3-26, *supra* note 77, at vi.

84. *Id.* at viii.

85. *See, e.g.*, S.C. Res. 1189, U.N. Doc. S/RES/1189 (Aug. 13, 1998) (sanctions imposed following terrorist bombings in Kenya and Tanzania).

86. Schmitt, *Responding to Transnational Terrorism under the* Jus Ad Bellum, *supra* note 52, at 2–5. *See also* Watts, *supra* note 52, at 64–65; North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243; William Howard Taft IV, *The Bush (43rd) Administration, in* SHAPING FOREIGN POLICY IN TIMES OF CRISIS: THE ROLE OF INTERNATIONAL LAW AND THE STATE DEPARTMENT LEGAL ADVISOR 127, 128–29 (Michael P. Scharf & Paul R. Williams eds., 2010) ("[We] had no difficulty in establishing that we had a right to use force in self-defense against Al-Qaeda and any government supporting it . . . .").

acts"[87] and commended all States to take necessary steps to prevent terrorism and ensure that terrorist acts are established as criminal offenses in domestic laws. Resolution 1373 also obliged member States to prevent the financing of terrorism; criminalize the collection of funds for terrorist purposes; freeze the financial assets of anyone who participates in, or facilitates, terrorism; take any steps necessary to prevent terrorist acts, including passing early-warning information to other States; suppress recruitment of members of terrorist groups; eliminate the supply of weapons to terrorists; deny safe haven to those involved in terrorism; and ensure that serious criminal penalties are established for all terrorist acts.[88]

In 2006 the General Assembly adopted the Global Counter-Terrorism Strategy and embraced what it called a common framework to fight terrorism.[89] The General Assembly recognized that counterterrorism law incorporates a multifaceted set of tools that relies on the legal principles in LOAC, human rights law, refugee and asylum law, and criminal law, along with the Charter, to constitute its framework.[90] Despite the aspirations of the General Assembly, however, more recently the World Justice Project agreed that "there is as yet no fully coherent international legal regime governing terrorism and responses to terrorism."[91] Although counterterrorism law has developed in recent years, the World Justice Project is correct, and the high visibility of cyber threats may provide incentives to further develop counterterrorism law as a set of international law norms.

In practice, counterterrorism law has evolved as something of a hybrid species of law, blending parts of conventional domestic criminal laws and procedures with modified LOAC principles, components of human rights

87. S.C. Res. 1373, *supra* note 53.

88. *Id.* Resolution 1373 has been described as "one of the most comprehensive and far-reaching resolutions adopted in the history of the Security Council." Curtis A. Ward, *Building a Capacity to Combat International Terrorism: The Role of the United Nations Security Council*, 8 JOURNAL OF CONFLICT AND SECURITY LAW 289, 298 (2003).

89. G.A. Res. 60/288, U.N. Doc. A/RES/60/288 (Sept. 8, 2006) (reviewed by the U.N. General Assembly biennially in G.A. Res. 62/272, U.N. Doc. A/RES/62/272 (Sept.5, 2008); G.A. Res. 64/297, U.N. Doc. A/RES/64/297 (Sept. 8, 2010); G.A. Res. 66/282, U.N. Doc. A/RES/66/282 (June 29, 2012)).

90. G.A. Res. 60/288, Action Plan: Preamble, Pillar IV, *supra* note 89, ¶¶ 2–5.

91. KATJA SAMUEL, NIGEL D. WHITE, ANA MARIA SALINAS DE FRÍAS, WORLD JUSTICE PROJECT COUNTER-TERRORISM EXPERT NETWORK, REPORT OF KEY FINDINGS AND RECOMMENDATIONS ON THE RULE OF LAW AND COUNTER-TERRORISM 12 (2012). The World Justice Project would locate the undefined remaining corpus of counterterrorism law in criminal laws. *Id.* at 56.

law, and refugee and asylum law.[92] By any standard, the evolution of counterterrorism law has not been easy or devoid of controversy. For example, over the last decade, opponents of U.S. domestic counterterrorism policies frequently argued that some of the measures taken, such as law of war detention and rendition, violated domestic law guarantees designed to protect criminal suspects. Our government responded that, in the ongoing counterterrorism campaign, the LOAC rules applied in a "new kind of war" and were being followed.[93] More recently, the counterterrorism targeted-killing policy initiated by the George W. Bush administration and expanded by President Obama remains controversial, in part because it reflects neither traditional law enforcement nor LOAC doctrines, but contains elements of both, and some components that are unique to counterterrorism.[94] More particularly, in the implementation of the targeting policy, positive identification of the target is required, although the lawful target is not a combatant in LOAC terms. The LOAC principle of distinction applies, and the military commander in charge of the targeting operation is instructed to capture the terrorist suspect if that option is available, so long as the suspect poses no imminent danger to the U.S. force or those around him. The targeting may occur wherever the target is found, but will not be carried out where law enforcement personnel are capable of interdicting the target using lawful means.[95]

In a similar vein, the 2006 Israeli Supreme Court *Targeted Killings* decision recognizes counterterrorism law as a distinct legal paradigm, in a sort of back-handed way. In the Court's opinion, instead of treating potential targets as either civilians or combatants according to the LOAC framework, the Court said that they are citizens sometimes taking part in hostilities, so that they may be targeted at only certain times.[96] Although the Israeli decision continues to focus on whether the government program involves law enforcement or military action and thus fails to acknowledge the

92. *See* Moeckli*, supra* note 71, at 168.

93. *See id.* at 164–65; Memorandum from Alberto R. Gonzales, Counsel to the President, Office of Counsel to the President, to George W. Bush, President of the United States, Decision re Application of the Geneva Convention on Prisoners of War to the Conflict with Al Qaeda and the Taliban (Jan. 25, 2002), *available at* http://www.torturingdemocracy.org/documents/20020125.pdf.

94. *See* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 376–410 (5th ed. 2011).

95. *Id.*

96. *See* Public Committee against Torture in Israel v. Government of Israel, HCJ 769/02, Judgment (Dec. 13, 2006), 46 INTERNATIONAL LEGAL MATERIALS 373 (2007), *available at* http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf.

range of counterterrorism components, the Court did recognize that the dichotomy between military action and criminal law enforcement is insufficient and that counterterrorism does not fit in either of those paradigms neatly or completely.

The 2010 U.S. Department of Defense Quadrennial Defense Review acknowledged that counterterrorism requires a "portfolio of capabilities,"[97] including gathering intelligence about terrorist suspects through a variety of human and technical means, apprehending persons believed to be connected with terrorist attacks, freezing terrorist financial assets and imposing other financial sanctions, interdicting illicit trafficking in weapons and drugs that furthers terrorism, patrolling borders and transit hubs, establishing regulatory best-practice standards for private-sector infrastructure, mounting counter-radicalization programs, and pursuing community resilience initiatives. The May 2011 White House International Strategy for Cyberspace declared that "the United States will defend its networks . . . from terrorists . . . and dissuade and deter those who threaten peace and stability through actions in cyberspace . . . with overlapping policies that combine national and international network resilience with vigilance and a range of credible defense options."[98]

The strategy treats cyber as an operational domain, like air, sea and land.[99] Applied to the cyber domain, counterterrorism law could support a variety of responses, including active defenses, other economic, intelligence and law enforcement operations, and kinetic responses, depending on the degree of harm caused by the attacks. Counterterrorism techniques in the cyber realm may include intelligence devices that locate and identify cyber terrorists and their equipment, information campaigns to counter terrorist propaganda, and techniques that seek to learn about and infiltrate illicit cyber activities and/or destroy the proliferation of cyber weapons and techniques. The final section takes a preliminary look at how counterterrorism law could contribute to the normative architecture for cyber war.

97. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 20 (2010).

98. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 41, at 12.

99. *Id.* at 6.

IV. *AD BELLUM* JUSTIFICATIONS FOR CYBER WAR—THE ROLE OF COUNTERTERRORISM LAW

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.

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.

At the same time that U.S. government lawyers and decision makers have been working to create a set of coherent and harmonious domestic and international legal prescriptions for high-profile security and counterterrorism operations abroad, such as detention and targeting,[100] the incredibly fast pace of evolving cyber war has quickly outstripped our capacity for building and implementing an integrated domestic and international law architecture. In other words, at a time when counterterrorism law is contested and in flux and cyber threats are emerging as a central national security concern, international lawmakers may benefit by dealing with the two spheres at the same time. We are playing from behind, doing our best working with LOAC, the Charter and operational law decisions. Fortunate-

100. *See* Robert M. Chesney, *Beyond the Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, xxx MICHIGAN LAW REVIEW (forthcoming 2013), draft *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138623.

ly, ongoing research supported by the Department of Defense's Minerva program at the Massachusetts Institute of Technology and Harvard on the development of cyber norms[101] and events such as the Naval War College/U.S. Cyber Command Conference on Cyber War and International Law that spurred this article can help to shore up the legal architecture for cyber war.

In some cyber war settings, the still-evolving counterterrorism law could provide the international law corpus with new norms that account for the unique qualities and challenges of cyber. Reconsider defensive cyber operations and the attribution problem. Given the practical difficulties in obtaining prompt attribution of incoming cyber attacks and further assuming that the speed of operations requires active defenses in the event of a destructive or highly disruptive cyber attack, the imminence requirement in self-defense may be modified to reflect the characteristics of cyber. Borrowing from the lessons of countering kinetic terrorism, imminence or immediacy may no longer be measured only as a function of time, but includes an additional consideration—when is the last opportunity to take action to thwart or blunt the attacks? Cyber attacks, like kinetic terrorism, arrive with no warning. Surprise is the attacker's asymmetric advantage in targeting the victim State. Depending on the gravity of the attack, the costs of waiting for the attack before responding may be unconscionably high. Nor is it reasonable to build into the calculus of cyber defense any expectation that cyber attackers will abide by legal requirements such as avoiding harm to civilians and their property.[102] As such, counterterrorism law could complement the evolving interpretation of Article 51 self-defense by developing a nuanced and context-specific normative base for responding to destructive or especially disruptive cyber attacks. The Charter framework could remain more closely aligned with its overarching military force orientation, and the new counterterrorism law could develop in ways that will be briefly explored in this section.

In 2004, the Berlin Declaration on Upholding Human Rights and the Rule of Law in Combating Terrorism of the International Commission of Jurists stated that "in adopting measures aimed at suppressing acts of terrorism, states must adhere strictly to the rule of law, including core principles of . . . international law. . . and, where applicable, humanitarian law.

101. *See* EXPLORATIONS IN CYBER INTERNATIONAL RELATIONS, http://ecir.mit.edu/research/publications (last visited Nov. 30, 2012).

102. *See* Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 16–20.

These principles . . . define the boundaries of permissible and legitimate state action against terrorism."[103]

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 road map for limiting cyber war.

In activating U.S. Cyber Command in 2010, the Department of Defense confronted congressional skepticism 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.[104] 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.[105] As this article 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 of the LOAC

---

103. INTERNATIONAL COMMISSION OF JURISTS (ICJ), THE BERLIN DECLARATION: THE ICJ DECLARATION ON UPHOLDING HUMAN RIGHTS AND THE RULE OF LAW IN COMBATING TERRORISM, at pmbl. (Aug. 28, 2004).

104. Ellen Nakashima, *Cyber Command Chief Says Military Computer Networks Are Vulnerable*, WASHINGTON POST, (June 4, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/06/03/AR2010060302355.html.

105. Watts, *supra* note 52, at 79 n.4. *See also id.* at 87 nn.139, 143.

bifurcation of international relations into states of war and 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.[106]

Starting with the text of the Charter, this article 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 similar response may not be considered an armed attack.[107] 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"[108] 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.

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.[109] In addition, under the terms of the Charter, forceful responses against non-State actors are handicapped at the outset because the

106. *Id.* at 60–61.

107. An Assessment of International Legal Issues, *supra* note 52, at 19.

108. Infamously included in Justice Potter Stewart's concurring opinion in *Jacobellis v. Ohio*, where Justice Stewart concluded that he could not further define the hard-core pornography at issue in the case, "[b]ut I know it when I see it." 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

109. An Assessment of International Legal Issues, *supra* note 52, at 16.

Charter was drafted to regulate relations among States. Still, for understandable reasons, States tend to defend all their uses of force as self-defense.[110] The reliance by the United States on self-defense in its targeting of terrorists outside traditional battlespaces 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.[111] As Sean Watts has warned, over time the written law of the Charter may take a backseat to the supposed law of self-preservation.[112] 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 if it is not possible or appropriate to respond by attacking the specific source of the computer attack, "any legitimate military target could be attacked . . . as long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to undertake them."[113] 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 has caused the United States to modify its long-standing views on the predicates for treating a cyber intrusion as an "armed attack" or "use of force." As Matt 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

110. Watts, *supra* note 52, at 87 n.142.
111. *Id.* at 76.
112. *Id.* at 87 n.143.
113. An Assessment of International Legal Issues, *supra* note 52, at 18.

armed attacks, while lower-level intrusions would enable cyber countermeasures in self-defense.[114] 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.[115] 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. Given 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.[116]

As has been widely noted over the last decade or more, the Charter in general and LOAC in particular are not optimally situated in every respect to regulate conflicts between States and terrorist organizations.[117] The State-centric orientation of the international legal instruments is based on a number of fundamental conceptions that do not apply easily in asymmetric conflicts with non-State terrorists—sovereignty and borders, declarations of war or armed conflict, protections for civilians and the disincentives to attack provided by State armies and weaponry.[118] Applied to cyber war, similar features stand out. States and sovereign borders are not significant barriers to Internet-based attacks. Most cyber attackers operate anonymously and are unannounced. Their victims may be governments, businesses and/or citizens, and attribution problems and the mobility of the terrorists' base of cyber war operations nearly eliminate the disincentives to attack. There are important differences between cyber attacks and other forms of terrorism, too. For example, most terrorist attacks produce immediately observable effects of physical violence, while cyber attacks may cause harm that is not easily seen.

As applied to cyber, the critique of the United States and a few other Western States for exporting their domestic counterterrorism policies in the service of a Global War on Terror may afford an opportunity for those

114. Waxman, *supra* note 39, at 439.

115. *Id.*

116. *Id.* at 443.

117. *See* NEW BATTLEFIELDS/OLD LAWS: CRITICAL DEBATES ON ASYMMETRIC WARFARE (William C. Banks ed., 2011).

118. *Id.*

same States to have something of a "do-over" in shaping cyber defense doctrines. Unlike al Qaeda attacks directed at the United States and a few Western European allies, cyber threats are more dispersed and widespread—consider the attacks on Georgia and Estonia in recent years. In addition to the major world powers, most States have a vested interest in arriving at a set of legal norms for defending against cyber attacks. Second, the norms that a still-maturing counterterrorism law could develop for cyber defense need not be threatening to the Charter or to the rule of law generally. The often expressed criticisms of the last decade that the United States was creating law-free zones in Guantanamo Bay or through its rendition practices[119] should not prejudice the development of new cyber law. New norms could be the product of national and international strategies and policies, tested over time through State practice, and not simply derived from existing legal doctrinal categories.[120] Unlike the post-9/11 policies, new counterterrorism cyber norms would not in every instance consist of extensions of the domestic laws of sponsoring States. For example, the fact that the customary law of countermeasures does not apply to interventions by non-State actors[121] exposes a gap in international law that an emerging cyber counterterrorism law could fill. Third, because the coherence of Charter- and LOAC-based international law as applied to cyber war really is in question, the opportunity for a scheme complementary to the Charter and LOAC is upon us or will soon be so.

Most new legal fields develop in response to new social or technological phenomena. Terrorism is anything but new. To be sure, the international networking of terrorists that led to the 9/11 attacks and others since is unprecedented, but domestic and international counterterrorism has occupied government and lawmaking agendas for nearly half a century. The international law of counterterrorism has been slow to develop, largely because of the politicization of the debate over definitions of what counts as terrorism and, as a consequence, which groups and activities may be countered with government-sanctioned programs. That the field is emerging internationally, despite the continuing wrangling over definitions, reflects the realization among States and the professionals in the field that maturing

119. *See*, e.g., Leila Sadat, *Extraordinary Rendition, Torture, and Other Nightmares from the War on Terror*, 75 GEORGE WASHINGTON LAW REVIEW 1200, 1226 (2007).

120. *See* Maggs, *supra* note 75, at 704.

121. *See supra* text accompanying note 24.

domestic counterterrorism law may be exported to the international community.[122]

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 counterterrorism law has developed normative principles—such as anticipatory self-defense—that accommodate these characteristics. By analogy counterterrorism 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 counterterrorism 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 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.[123] Counterterrorism 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.[124] The analogies to ongoing U.S. actions in its counterterrorism targeting program are striking.[125]

---

122. *See* Moeckli, *supra* note 71, at 173, 176–77; *see generally* GLOBAL ANTI-TERRORISM LAW AND POLICY, *supra* note 76.

123. *See* TALLINN MANUAL, *supra* note 13, rule 6.

124. The policy decision in such an instance may be based on different factors, of course, and may lead to decisions not to intervene where the law would permit the operation.

125. *See* Robert M. Chesney, *Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, 13 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 3 (2011).

Just as counterterrorism law is developing through an uneven process of fits and starts, missteps and recalibrations, it is likely that international law governing cyber war will emerge in a similar way, over time, as the product of State, regional and perhaps even global policies and strategies. First-generation counterterrorism law developed by analogy to decades of armed violence in the proxy wars fought during the Cold War. Secrecy was the norm, attribution was unofficial or non-existent and the *jus ad bellum* architecture was unclear at best. Indeed, controversy continues to surround State practice in certain counterterrorism policies, such as the shadow war being waged by the United States against al Qaeda and its affiliates in more than a dozen countries outside traditional battlespaces.[126]

Second-generation counterterrorism law is evolving now, a combination of exported second-generation domestic counterterrorism laws, some pertinent international treaties, bi- and multilateral agreements, and State practices that are maturing in responding to al Qaeda and other terrorist groups. Lessons have been learned from the proxy wars experience and from responding to terrorist attacks. Because terrorists' lack of attribution and surprise tactics require high levels of operational secrecy in counterterrorism, domestic legal reforms have moved toward greater regulation of intelligence operations, emphasizing the providing of information on intelligence operations to overseers, and an emphasis on positive identification of targets in potentially lethal counterterrorism operations.[127]

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. The growing capabilities for cyber sleuthing in the digital age suggest that development of a cyber-based intelligence law from a counterterrorism platform may be an important component of the architecture for twenty-first-century cyber war governance. 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

126. Scott Shane, Mark Mazzetti & Robert F. Worth, *Secret Assault on Terrorism Widens on Two Continents*, NEW YORK TIMES (Aug. 14, 2010), http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0.

127. *See* William C. Banks, *The United States a Decade After 9/11*, *in* GLOBAL ANTI-TERRORISM LAW AND POLICY, *supra* note 76, at 449, 450–51, 470–80.

involving military weapons systems constitutes armed aggression.[128] 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.[129] Yet intelligence collection is also at the center of counterterrorism, and likewise is subject to domestic legal controls, but no international legal regulation. 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 counterterrorism law for cyber operations may evolve through something like natural law–type or just war theory reasoning, as has been the case with the development of some other international law norms.[130] 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. Like counterterrorism law as developed and exported by the United States after 9/11, 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.[131] Ironically, as some prominent U.S. academics developed theories of "vertical domestication"[132] 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 mili-

128. *See* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 AIR FORCE LAW REVIEW 217, 223–24 (1999).

129. *See* TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 261, 263.

130. *See* Jeffrey L. Dunoff & Mark A. Pollack, *What Can International Relations Learn from International Law?* 11 (Temple University Legal Studies Research Paper No. 2012-14, 2012), http://ssrn.com/abstract=2037299.

131. See the description of the process in W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 82 (2003).

132. Harold Hongju Koh, *The 1998 Frankel Lecture: Bringing International Law Home*, 35 HOUSTON LAW REVIEW 623, 626–27 (1998) (citing Harold Hongju Koh, *Transnational Legal Process*, 75 NEBRASKA LAW REVIEW 181, 183–84 (1996)).

tary detention and the use of military commissions.[133] Other States may develop counterterrorism legal authorities in this emerging paradigm of cyber war through a similar process.

However it occurs, counterterrorism 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 counterterrorism law regime may enable victim States with 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 counterterrorism 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.[134]

For the United States, the fact that so much of our infrastructure is privately owned makes securing the infrastructure legally and practically problematic,[135] 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"[136] 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 is consistent with its long-standing opposition to some other States' expansive interpretations of Articles 2(4) and 51 to include econom-

133. Banks, *supra* note 127, at 478–80; Robert M. Chesney, *Who May Be Held? Military Detention Through the Habeas Lens*, 52 BOSTON COLLEGE LAW REVIEW 769 (2011).

134. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 245.

135. Waxman, *supra* note 39, at 451.

136. *Id.* at 452.

ic coercion and political subversion.[137] 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 twenty-five years show, 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. Relying on a developing counterterrorism law to embody the cyber doctrines internationally would thus serve the ancillary goal of retaining the traditional military force core of the bookend Charter provisions. Not that such a legal code of conduct based in counterterrorism 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.[138]

National policies and operational practices will lead us toward a supplemental cyber law. Consider an illustration from counterterrorism law that developed in the carrying out of kinetic operations by the U.S. military in recent years when U.S. forces pursue a lawful target in a counterterrorism operation. As highlighted by the raid that killed Osama bin Laden in 2011, the operational standard includes a "kill or capture" option, deferring to commanders on when a capture may reasonably be accomplished. Under the Charter and LOAC, once a lawful target has been positively identified, the use of lethal force without further deliberation is lawful. The theoretically more human rights–oriented operational law, driven by counterterrorism policy, is becoming part of international counterterrorism law through State practice. In fact, operational law and military service lawyers have taken on a central role in military decision making and thus in the shaping of State practice, especially after 9/11.[139] Cyber law in counterterrorism may develop in much the same way, based on operational rules and State practice that tailor the legal norms to requirements.[140]

---

137. *Id.* at 453.

138. *Id.* at 455–57.

139. *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 122–60 (2012).

140. *See* Ian Hurd, *Is Humanitarian Intervention Legal? The Rule of Law in an Incoherent World*, 25 ETHICS AND INTERNATIONAL AFFAIRS 293 (2011) (noting the dynamic relation-

V. 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 backup 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.[141] 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 backup 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 predetermined 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.

---

ship between State practice and international law where humanitarian intervention may be legally plausible despite Article 2(4)).

141. *See* BRENNER, *supra* note 3, at 96–97 (describing SCADA systems).

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 situated in South Asia, what law governs the response? This article 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,[142] Stuxnet created the precedent, as did Israel's cyber attack on Syrian air defenses when it attacked a suspected Syrian nuclear site in 2007,[143] Russia's cyber attacks in its dispute with Georgia[144] and the apparent use of cyber weapons by the United States to target al Qaeda websites and terrorists' cell phones.[145] Now that the cyber war battlefield apparently has expanded to Beirut banks and a neutral State,[146] 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 in determining what kinds of cyber attacks trigger the authority to take defensive actions and the nature of the defenses that will be permitted. The facts needed to make the normative

142. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, NEW YORK TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

143. David A. Fulghum, Robert Wall & Amy Butler, *Cyber-Combat's First Shot: Attack on Syria Shows Israel is Master of the High-Tech Battle,* AVIATION WEEK & SPACE TECHNOLOGY, Nov. 26, 2007, at 28.

144. John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES, Aug. 12, 2008, at A1.

145. *See supra* notes 11–12; Jack Goldsmith, *Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya*, LAWFARE (Oct. 18, 2011, 7:48 AM), http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/.

146. Katherine Mayer, *Did the Bounds of Cyber War Just Expand to Banks and Neutral States?*, THE ATLANTIC, Aug. 21, 2012, http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/#.UDPjrcFCPJo.email.

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.[147] 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.

This article 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.[148] 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.[149]

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 by product 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.[150] If States or the international community attempts 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. Counterterrorism law could support or help build the normative architecture for cyber operations, at least at the margins, where the legal landscape

147. *See* Waxman, *supra* note 39, at 448.

148. MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 69–70 (2009); O'Connell, *supra* note 20.

149. *See* Waxman, *supra* note 39, at 446–47.

150. *See* TALLINN MANUAL, *supra* note 13, rule 9, cmts. 10 & 12 (reviewing the "plea of necessity" recognized in Article 25 of the Articles on State Responsibility).

is not now clear. Over time a cyber regime may develop that 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.[151] The Charter and LOAC do not have all the answers, and cyber is not fundamentally a military problem.

151. I am indebted to General Ken Watkin, Canadian Forces (Ret.), for reminding me of the relevance of the adage.