INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

International Law and Cyber Threats from Non-State Actors

Laurie R. Blank

89 INT'L L. STUD. 406 (2013)

Volume 89 2013

International Law and Cyber Threats from Non-State Actors

Laurie R. Blank[*]

I. INTRODUCTION

The so-called "virtual" world, that of the Internet, computer networks and cyberspace in general, is now very firmly part of the "real world," especially in the areas of national security and military strategy. Revolutionary advances in technology now enable both militaries and civilians to engage in cyber activity to achieve objectives, whether related to protest and revolution, crime, terrorism, espionage or military operations. At one end of the spectrum both governments and private companies face a nearly constant onslaught of cyber activity seeking to access information, undermine or damage systems, or otherwise gain a financial, political or strategic advantage of some kind. At the other end of the spectrum are acts that some commentators call "cyber war" or "cyber attacks," including the cyber operations in Georgia during the 2008 conflict between Russia and Georgia, the Stuxnet virus or the comprehensive computer network operations launched against the Estonian government in the summer of 2007. Governments and companies alike have established both formal and informal mechanisms for countering these rapidly developing threats and operations in cyberspace, including, for example, U.S. Cyber Command, China's Peo-

* Director, International Humanitarian Law Clinic, Emory University School of Law.

ple's Liberation Army General Staff Department's 3rd Department, Iranian Sun-Army and Cyber Army, Israel's Unit 8200, and the Russian Federal Security Service's 16th Directorate.

Rhetoric has matched these developments as well. We now read about a wide range of cyber "things:" cyber crime, cybersecurity, cyber espionage, cyber threats, cyber attacks, cyber war or warfare, cyber terrorism and so on. A look at news coverage of these issues in recent years demonstrates the growing focus across a range of countries, industries and disciplines, with the number of news stories mentioning either "cyber war," "cyber warfare" or "cyber attack" in 2010 or 2011 more than triple that of any previous year before 2009.[1] The number of scholarly articles, academic conferences, policy discussions and other events addressing cyber issues is further evidence of the extent of the current discourse.

Within the realm of law applicable to and governing cyber activity, a host of legal regimes are relevant, including, most notably, domestic criminal law, national security law and international law. Just as examples, the U.S. Congress has engaged in extensive debate over various forms of cybersecurity legislation[2] and international experts have devoted—and continue to devote—significant energy to examining the extent and nature of the application of international law to cyber war and related activities.[3] In addition, the nature of cyber operations, computer networks, the Internet and related components of the cyber arena mean that a veritable plethora of actors are and can be involved in cyber activities. Among these are militaries, other government agencies, private companies, terrorist groups and individuals acting on a range of different motivations, often referred to as "hacktivists." The nature of today's globalized and interconnected world combined with the extensive reliance on technology, computer systems and Internet connectivity means that non-State actors, whether individuals or groups of some kind, can have a significant impact through cyber activity.

---

1. A brief Lexis-Nexis search of major newspapers shows 944 and 965 hits for the term "cyber attack" in 2010 and 2011, respectively, compared to approximately 200 or fewer for any year before 2009. The same general pattern holds true for the terms "cyber war" and "cyber warfare." Based on the first few months of 2012, news coverage looks to be comparable to that of the previous two years.

2. *See, e.g.*, Paul Rosenzweig, *The Politics of the Cyber-Legislation Debate*, LAWFARE (Apr. 19, 2012, 11:48 AM), http://www.lawfareblog.com/2012/04/the-politics-of-the-cyber-legislation-debate/.

3. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

At the same time, the complexity of cyber operations—in terms of characterizing the nature of the operations, identifying the main players and developing appropriate options in response—opens up an equally complex legal environment for analyzing the parameters of and framework for such responses. This legal environment includes the law of armed conflict (LOAC), the law governing the resort to force *(jus ad bellum)* and human rights law, along with national security law and domestic criminal law. Cyber operations can be used both in armed conflict and in the absence of armed conflict, which is, of course, part of the complex nature of the legal inquiry. A host of interesting questions arise from the use of cyber capabilities by States and non-State actors, including when cyber acts trigger the international law regime governing the use of force and/or LOAC and the nature of self-defense in response to cyber acts, in particular, against non-State actors, and the contours of a cyber battlespace, to name a few. Furthermore, both *jus ad bellum* and LOAC pose challenging questions regarding the appropriate application of the law and the parameters of the legal paradigm at issue. This article will focus on the international legal framework that governs defense against cyber threats from non-State actors, specifically LOAC and the law governing the resort to force. In doing so, it will identify both essential paradigms for understanding options for response to cyber threats from non-State actors and key challenges in those paradigms. Section II addresses *jus ad bellum* and how it applies to and provides guidance for State responses to cyber actions by non-State actors. Section III analyzes when and how LOAC applies to non-State cyber acts and examines some of the specific challenges cyber acts pose for such analysis. Finally, Section IV highlights broader crosscutting issues, such as the challenges of multiple overlapping legal paradigms and the role and power of rhetoric, in exploring how States can and do respond to cyber threats from non-State actors.

The current discourse about cyber war suggests a look back at the discourse surrounding appropriate responses to terrorist attacks and terrorist groups in the aftermath of the September 11 attacks. Questions abounded, for example, regarding whether responses to terrorists fell within a law enforcement paradigm or a war paradigm, whether the same international law that governed hostilities and law enforcement in other situations should also guide responses to terrorists, and whether terrorists were entitled to basic rights under either human rights law or LOAC. The debate and discourse about cyber war are in many ways wholly different: extensive legal analysis and debate are preceding action and few commentators or policy-

makers are proposing that cyberspace be a "law-free" arena. However, some aspects of the past decade of debate over lawful counterterrorism policy offer useful lessons for exploring the legal regime governing cyber operations, including the role of rhetoric and the need to understand the interplay between multiple overlapping legal frameworks.

As a preliminary matter, it is useful to note that cyber activities take place along an expansive continuum with information analysis and gathering at one end and hostilities at the other, roughly, and including espionage, surveillance, crime and other activities along its span. In many cases, it is likely that groups or individuals will engage in operations that fall within more than one category along that continuum, thus triggering potential application of multiple legal frameworks. Terrorist attacks pose many of the same challenges. A terrorist attack is, at a minimum, a crime, but over the past decade it has become accepted fact that terrorist attacks can also be hostilities that constitute an armed conflict. As a result, policymakers and academics have engaged in extensive debate regarding whether responses to terrorism fall within a law enforcement paradigm or a war paradigm. Although the full parameters of that debate are outside the scope of this article, the debate itself offers useful lessons in recognizing the multiple legal paradigms applicable to cyber activities and analyzing how and in what situations they apply. Throughout the analysis, therefore, this article will often refer to existing and developing considerations in responses to non-State terrorist entities, both in rhetoric and in policy and legal choices, as appropriate in examining the legal paradigms for responding to cyber threats from non-State actors.

II. THE LAW GOVERNING THE RESORT TO FORCE

In many cases, the cyber activity of non-State actors falls squarely within a broad category of cyber crime, but perhaps can also be categorized as cyber espionage. Some acts, however, pose a threat not just to private companies or industry, but in a more comprehensive way to the national security of the State. Cyber warfare thus has been defined broadly to include, among other actions, defending information and computer networks, deterring information attacks, denying an adversary's ability to defend networks and deter attacks, engaging in offensive information operations against an ad-

versary and dominating information on the battlefield.[4] The transition from domestic and cross-border law enforcement to more forceful responses depends on an analysis of how and when international law establishes a right for States to use force and in what manner. The increasing focus on cyber operations by both States and non-State actors has led to an extensive discourse on the question of when an action in the cyber realm constitutes a use of force,[5] a key preliminary question in any discussion regarding the legality of the use of force in the cyber arena. This article, which focuses specifically on responding to non-State actors in the cyber realm, will use that discourse as a backdrop, but will not delve into a discussion of what constitutes a use of force generally for the purposes of *jus ad bellum*. Rather, since there is extensive scholarship on the question of what cyber activity constitutes a use of force,[6] the instant discussion will assume the existence of a use of force and proceed to the next step in the legal analysis. Furthermore, this article will not address the legal questions surrounding when a State may attribute the acts of a non-State actor to a State for the purposes of responding to threats or attacks by using force against that State.

Jus ad bellum is the Latin term for the law governing the resort to force—that is, when a State may use force within the constraints of the United Nations Charter framework and traditional legal principles. The modern *jus ad bellum* has its origins in the 1919 Covenant of the League of Nations, the 1928 Kellogg-Briand Pact and the United Nations Charter.[7] In particular, Article 2(4) of the United Nations Charter prohibits the use of force by one State against another: "All members shall refrain in their in-

---

4. *See* STEPHEN HILDRETH, CONGRESSIONAL RESEARCH SERVICE, RL30735, CYBERWARFARE 16–17 (2001), *available at* http://www.fas.org/irp/crs/RL30735.pdf.

5. *See* 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 (1999); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STANFORD JOURNAL OF INTERNATIONAL LAW 207 (2002); 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 (2011); Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm*, 37 WILLIAM MITCHELL LAW REVIEW 5049 (2011); Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 59 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); Matthew Hoisington, *Note: Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 BOSTON COLLEGE JOURNAL OF INTERNATIONAL LAW 439 (2009).

6. *See, e.g.*, Schmitt, *supra* note 5; Jensen, *Computer Attacks on Critical National Infrastructure*, *supra* note 5; Waxman, *supra* note 5.

7. MALCOLM N. SHAW, INTERNATIONAL LAW 780–81 (4th ed. 1997).

ternational relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[8] This provision, by placing severe restrictions and prohibitions on the use of force, is in many ways the foundation of the UN's goal of "sav[ing] succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind."[9]

The Charter provides for three exceptions to the prohibition on the use of force, each of which is relevant to cyber operations in response to a threat from a non-State actor. First, a State may use force with the consent of the territorial State, such as when a State battling a rebel group requests assistance from one or more other States. In such cases, the territorial State can only consent to such assistance and uses of force in which it could legally engage—no State can consent to actions by another State that would violate international law if undertaken by the requesting State. To the extent that a State engages in cyber operations that rise to the level of a use of force in such a context, it would thus need to ensure that such use of force remained within the parameters of actions the territorial State could lawfully undertake. Second, a State can use force as part of a multinational operation authorized by the Security Council under Chapter VII, as provided in Article 42.

Third, a State may use force in accordance with the inherent right of self-defense under Article 51 in response to an armed attack. This provision builds on and establishes the basic framework of the *jus ad bellum*, stating: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[10] It is in this context that most issues and considerations regarding defense against cyber threats from non-State actors will arise. As a result, it is helpful to first set forth the basic contours of international law with regard to the use of force in self-defense.

The classic formulation of the parameters of self-defense stems from the *Caroline* incident. British troops crossed the Niagara River to the American side and attacked the steamer *Caroline*, which had been running arms and materiel to insurgents on the Canadian side. The British justified the

8. U.N. Charter art. 2, para. 4.
9. *Id.*, pmbl.
10. *Id.*, art. 51.

attack, in which they set fire to the *Caroline* and killed one American, on the grounds that their troops had acted in self-defense. In a letter to his British counterpart, Lord Ashburton, U.S. Secretary of State Daniel Webster declared that the use of force in self-defense should be limited to "cases in which the 'necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'"[11] Furthermore, the force used must not be "unreasonable or excessive; since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."[12] Much of the extensive literature analyzing the right of self-defense, and, in particular, the parameters of the right of self-defense in response to terrorist attacks,[13] offers a useful foundation for the instant analysis.

A. The Right to Respond to Cyber Threats from Non-State Actors

A State that faces cyber threats from or attacks by non-State actors can respond as long as the response is lawful within the context of the *jus ad bellum*. Any lawful use of force in self-defense depends initially on the existence of an armed attack. Note that an armed attack is more severe and significant than a use of force, meaning that a State can be the victim of a

---

11. Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, Special British Minister (Aug. 6, 1842), *in* 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW § 217 at 412 (1906).

12. Letter from Daniel Webster, U.S. Secretary of State, to Henry Fox, British Minister in Washington (Apr. 24, 1841), *in* 29 BRITISH & FOREIGN STATE PAPERS 1840–1841, at 1138 (1857).

13. *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 175–82 (2d ed. 1994) (discussing the concept and right of self-defense); David Kretzmer, *Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?*, 16 EUROPEAN JOURNAL OF INTERNATIONAL LAW 171, 173 (2005) (noting that some States argue that targeted killings are within the "state's inherent right to self-defence"); Craig Martin, *Going Medieval: Targeted Killing, Self-Defence, and the* Jus ad Bellum *Regime*, *in* TARGETED KILLINGS: LAW & MORALITY IN AN ASYMMETRICAL WORLD 223 (Claire Finkelstein, Jens David Ohlin & Andrew Altman eds., 2012) (discussing the validity of a self-defense claim regarding targeted killing of suspected terrorists); Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 JOURNAL OF TRANSNATIONAL LAW & POLICY 237 (2010) (arguing that self-defense is permissible against non-State actors who commit armed attacks and that actions of self-defense can be made in another State without that State's consent); Michael N. Schmitt, *Responding to Transnational Terrorism Under the* Jus ad Bellum*: A Normative Framework*, 56 NAVAL LAW REVIEW 1 (2008) (noting that the "United States claim[ed] self-defense as a right in forcefully countering terrorism").

use of force without being the victim of an armed attack that triggers the right of self-defense.[14] In assessing whether a particular hostile action directed at a State rises to the level of an armed attack, the International Court of Justice (ICJ) looks at the scale and effects of the act.[15] For example, if a State deploys its regular armed forces across a border, that will generally be considered an armed attack, as will a State's sending irregular militias or other armed groups to accomplish the same purposes. In contrast, providing weapons or other assistance to rebels or other armed groups across State borders will not reach the threshold of an armed attack.

Directly related to the analysis of self-defense against cyber threats or attacks by non-State actors, a key *jus ad bellum* question is whether only States can launch an armed attack. Nothing in Article 51 specifies that the right of self-defense is only available in response to a threat or use of force by another State. Nonetheless, the precise contours of what type of actor can trigger the right of self-defense remains controversial. Some argue that only States can be the source of an armed attack—or imminent threat of an armed attack—that can justify the use of force in self-defense.[16] The ICJ has continued to limit the right in this manner in a series of cases.[17] However, State practice in the aftermath of the 9/11 attacks provides firm support for the existence of a right of self-defense against non-State actors, even if unrelated to any State.[18] Indeed, the *Caroline* incident, which forms

---

14. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 191 (June 27) [hereinafter *Military and Paramilitary Activities*]. *See also* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict*, *in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 163 (2010), *available at* http://books.nap.edu/openbook.php?record_id=12997&page=R1.

15. *Military and Paramilitary Activities*, *supra* note 14.

16. *See, e.g.*, Antonio Cassese, *The International Community's "Legal" Response to Terrorism*, 38 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 589, 597 (1989); Eric Myjer & Nigel White, *The Twin Towers Attack: An Unlimited Right to Self-Defense*, 7 JOURNAL OF CONFLICT AND SECURITY LAW 5, 7 (2002) ("Self-defense, traditionally speaking, applies to an armed response to an attack by a state.").

17. *See, e.g.*, *Military and Paramilitary Activities*, *supra* note 14; Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 (Dec. 19); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 215 (July 9).

18. *See, e.g.*, DINSTEIN, *supra* note 13, at 214; Christopher Greenwood, *International Law and the Preemptive Use of Force: Afghanistan, al Qaeda, and Iraq*, 4 SAN DIEGO INTERNATIONAL LAW JOURNAL 7, 17 (2003) (discussing the effects of attacks made by non-State

the historical foundation of the right to self-defense, involved an armed attack by non-State actors. UN Security Council Resolution 1368, for example, recognized the inherent right of self-defense against the September 11 attacks and "[u]nequivocally condemn[ed] in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and *regard[ed]* such acts, like any act of international terrorism, as a threat to international peace and security."[19] Similarly, the North Atlantic Council issued a statement activating the collective self-defense provision in Article 5 of the North Atlantic Treaty, as did the Organization of American States regarding its constituent treaty.[20] Several other States have asserted the same right, including Turkey, Israel, Colombia and Russia.[21] Over the past decade, the challenge of responding to transnational terrorism has helped drive State practice and debate regarding the lawfulness of self-defense in response to armed attacks by non-State actors.

Although the analysis may seem relatively straightforward in the con-

---

actors); Sean D. Murphy, *The International Legality of US Military Cross-Border Operations from Afghanistan into Pakistan*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 109, 126 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies) ("While this area of the law remains somewhat uncertain, the dominant trend in contemporary interstate relations seems to favor the view that States accept or at least tolerate acts of self-defense against a non-State actor."); Raphaël Van Steenberghe, *Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?*, 23 LEIDEN JOURNAL OF INTERNATIONAL LAW 183, 184 (2010) (concluding that recent State practice suggests that attacks committed by non-State actors alone constitute armed attacks under Article 51).

19. S.C. Res. 1368, ¶ 1, U.N. Doc. S/RES/1368 (Sept. 12, 2001) (emphasis added).

20. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; 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; Inter-American Treaty of Reciprocal Assistance art. 3.1, Sept. 2, 1947, 62 Stat. 1681, 1700, 21 U.N.T.S. 77, 93; Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs Acting as Organ of Consultation in Application of the Inter-American Treaty of Reciprocal Assistance, OEA/Ser.F/II.24, RC.24/RES.1/01 (Sept. 21, 2001). Similarly, Australia activated the collective self-defense provision of the ANZUS Pact. Security Treaty Between Australia, New Zealand and the United States of America art. IV, Sept. 1, 1951, 3 U.S.T. 3420, 3423, 131 U.N.T.S. 83, 86; Brendan Pearson, *PM Commits to Mutual Defence,* AUSTRALIAN FINANCIAL REVIEW, Sept. 15, 2001, at 9.

21. For an extensive treatment and discussion of the use of force in self-defense and State practice, see Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012).

text of military units, armed bands and kinetic force, in the cyber realm, identifying and analyzing an armed attack are significantly more challenging. The most common method of analysis with regard to whether cyber actions rise to the level of an armed attack is an effects-based analysis. At present, there is a general consensus that "any use of force that injures or kills persons or damages or destroys property" constitutes an armed attack, including in the cyber arena.[22] Others point to the target of a cyber operation, arguing that any cyber action against critical national infrastructure should qualify as an armed attack,[23] or, alternatively, to an "instrument-based" approach, according to which a cyber operation constitutes an armed attack if "the damage caused by a cyber attack could previously have been achieved only by a kinetic attack."[24] In contrast, economic damage, political embarrassment or coercion, a disruption of communications, and the distribution of propaganda through cyber means do not rise to the level of an armed attack. The *Tallinn Manual on International Law Applicable to Cyber Warfare* explains that cyber intelligence gathering and theft do not constitute an armed attack, nor would "cyber operations that involve brief or periodic interruption of non-essential cyber services."[25]

Responding to cyber threats or attacks by non-State actors within this paradigm poses several challenging questions beyond the characterization of an armed attack or the continued—although waning—uncertainty regarding whether non-State actors could alone launch an armed attack that triggers the right of self-defense. The first such question stems from one of the fundamental challenges of cyber activity: attribution. Identifying the source of an attack is a uniquely complex and difficult act in the cyber arena; these challenges add an additional layer of legal uncertainty in analyzing a State's right to respond in self-defense. Although general consensus exists, particularly in the discourse on cyber warfare, that attacks by non-State actors (those not related or attributable to a State) can trigger the right of self-defense,[26] what about a lone wolf actor? Or a loosely knit group of hacktivists? The traditional notion of a non-State actor launching an armed

22. TALLINN MANUAL, *supra* note 3, at 54.

23. Jensen, *Computer Attacks on Critical National Infrastructure*, *supra* note 5 at 221–26.

24. David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 91 (2010) (citing Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 103–5 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies)).

25. TALLINN MANUAL, *supra* note 3, at 55.

26. *Id.* at 57.

attack on a State conjures images of rebel groups or guerrilla fighters—some type of organized entity with a name, a structure and, likely, some method of directing operations.[27] Cyber warfare in particular raises the specter of a solo actor, or perhaps a small handful of actors, who can pose a devastating threat to a State through a cyber attack. In the absence of evidence linking an individual or individuals to a State or a larger, more organized entity, it is unclear whether such an attack falls within the right of self-defense or would remain, in essence, in the criminal arena. Counterterrorism does offer some useful analogies in this respect, particularly in the current environment of attacks conducted against terrorist operatives in far-flung regions of Pakistan and Yemen. The United States relies on self-defense as one primary justification for the use of force against terrorist operatives;[28] however, it always presents the target as a member of al Qaeda or affiliated terrorist groups, thus not offering any firm evidence of the use of force against a solo actor. Nonetheless, it is not inconceivable—although it is perhaps highly unlikely—that the United States or other State actor might argue that force is the only recourse to repel or deter an armed attack by a lone-wolf actor in a particular circumstance.

Attribution poses a second challenge as well. In using force in self-defense against a non-State actor, the State using force will be doing so in the territory of another State, one that did not launch the original attack and does not bear direct responsibility for the attack. The responding State must, therefore, act either with the consent of the territorial State or on the grounds that the territorial State is unwilling or unable to take action to remove the threat posed by the non-State actor and prevent future attacks.[29] The notions of unwilling or unable are not necessarily fully defined in the realm of kinetic attacks, and attribution challenges make them much harder to apply in the cyber arena. At the preliminary level, the inherently obscure nature of cyber activities can make it difficult to tell the specific location from which the attack emanated—including which State—thus undermining the ability to use the unwilling or unable formulation as a foundation

---

27. *See infra* pp. 428 - 429 for a more detailed discussion of the notion of an organized armed group within the cyber context.

28. Harold Hongju Koh, Legal Adviser, U.S. Department of State, *Keynote Address at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law* (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm. *See also* Laurie R. Blank, *Targeted Strikes: The Consequences of Blurring the Armed Conflict and Self-Defense Justifications*, 38 WILLIAM MITCHELL LAW REVIEW 1655 (2012).

29. *See generally* Deeks, *supra* note 21 (examining in depth the historical and legal foundations of the "unwilling or unable" test).

for responsive action. In this respect, cyber poses perhaps unique challenges because of the ability to dissemble and present an attack as coming from one or more different States or locations, or simply because an attack passes through or can be traced back to multiple—even over a hundred—States.[30] For this reason, the victim State must tread carefully and seek as much clarity regarding the source of the attack as possible to avoid launching a self-defense response in the wrong direction. This challenge is particularly acute with regard to responding to attacks by non-State actors unaffiliated with a State because there may well be fewer accountability trails to follow or venues for attributing responsibility.

Finally, the cyber arena is particularly relevant to the question of whether a series of lower-level attacks or incidents can combine together to rise to the level of an armed attack that triggers the right of self-defense. Some argue that "gaps in [*jus ad bellum*'s] response structure will prove highly susceptible to low-intensity cyber attacks, leaving victim States to choose between enduring damaging intrusions and disruptions or undertaking arguably unlawful unilateral responses."[31] In effect, because of the distinction between a mere use of force, which does not trigger the right of self-defense, and the more significant armed attack, which does trigger that right, there is fertile ground for extensive and disruptive cyber activity that does not necessarily provide the victim State with significant opportunities for a useful response. Here, attribution plays a key role again. To the extent that a State can determine that a series of low-level cyber incidents originate from the same source—the same non-State actors or entity—then there is a strong argument to be made that, taken together, the incidents constitute an armed attack to which the State can lawfully respond in self-defense.[32]

B. The Nature of Responses to Cyber Attacks by Non-State Actors

If a State has been the victim of a cyber event that meets the threshold for an armed attack, it can, under the *jus ad bellum*, respond with force in self-

30. For example, the distributed denial of service attacks on Estonia in 2007 were ultimately traced back to over 178 States. *See* Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, ATLANTIC COUNCIL (Jan. 2012), https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf.

31. Sean Watts, *supra* note 5, at 60–61.

32. TALLINN MANUAL, *supra* note 3, at 55 (noting also that this approach is called the "pin-prick theory" or the "accumulation of effects theory").

defense. In so doing, the State must comport with the requirements of necessity, proportionality and immediacy.[33] As a first step, the law does not constrain a State responding to a cyber attack to use only cyber force in response. The victim State can use kinetic force in self-defense as a response to a cyber attack if that use of kinetic force comports with the requirements of necessity and proportionality.

The requirement of necessity addresses whether there are adequate non-forceful options to deter or defeat the attack, such as diplomatic avenues, defensive measures to halt any further attacks or reparations for injuries caused. Necessity includes not only action taken to halt and defeat an initial attack, but broader action to eliminate a continuing threat. More specifically, in the cyber realm, necessity requires an understanding of the ability to achieve the desired end to the threat or attack using a range of options in both the cyber and non-cyber arenas. Thus, if an armed attack by a non-State actor exposes and takes advantage of a particular vulnerability in a State's cyber defenses that can then be repaired to deny further cyber incursions, such bolstering of defenses might be a sufficient non-forceful alternative, making the use of force unlawful. In the case of attacks by non-State actors, States seeking to act in self-defense must first explore whether the territorial State can take action to stop the non-State actors from launching further attacks, including, potentially, detention of those responsible, as part of determining whether there are any non-forceful alternatives available. As noted above, the attribution challenges inherent in cyber activity can make this aspect of the *jus ad bellum* difficult to analyze.

The requirement of proportionality measures the extent of the use of force against the overall military goals, such as fending off an attack or subordinating the enemy. Rather than addressing whether force may be used at all—which is the main focus of the necessity requirement—proportionality looks at how much force may be used. In doing so, proportionality focuses not on some measure of symmetry between the original *attack* and the use of force in response, but on whether the measure of counterforce used is proportionate to the needs and goals of *repelling* or *deterring* the original attack.[34] The force used may indeed be significantly

33. These obligations form part of customary international law and have been reaffirmed numerous times by the International Court of Justice. *See, e.g.*, *Military and Paramilitary Activities*, *supra* note 14, ¶¶ 176, 194; Oil Platforms, *supra* note 17, ¶¶ 43, 73–74, 76; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8) [hereinafter *Nuclear Weapons*].

34. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 237 (4th ed. 2005).

greater than that used in the attack that triggered the right to self-defense—what matters is the result sought, not the equivalence between attack and response. For this reason, there could be circumstances in which kinetic force is an appropriate—that is, proportionate—response to a cyber attack, even though it appears, at first blush, to be force of an entirely different nature from that used in the initial attack.[35] This can be especially true in examining a State's response to a cyber attack by a non-State actor. The non-State actor simply may not be vulnerable to cyber force in the same manner as a State with its critical infrastructure and national security considerations. The use of cyber force against that non-State actor may not have the desired effect of repelling the attack or deterring the non-State actor from continuing the attack or launching additional attacks because it cannot cause sufficient consequences in that scenario. Kinetic force is, under these circumstances, more likely to have that effect and be able to achieve the goal of ending the attack(s).

The final requirement for the lawful use of force in self-defense is immediacy. In the case of a response to an ongoing attack, immediacy is not relevant—necessity and proportionality will dominate the analysis of whether the use of force is appropriate. Immediacy considerations arise when a State uses force in self-defense in advance of an attack or long after an attack is over. In the latter case, a forceful response long after an attack will no longer serve defensive purposes, but will be retaliatory, and therefore unlawful. The first scenario is often termed anticipatory self-defense—the use of force to prevent an imminent attack and the death and damage it will cause. As in other components of the *jus ad bellum* analysis, cyber activity poses some unique considerations with regard to the requirement of immediacy. In many cases, the instantaneous nature of cyber operations means that the immediacy requirement is effectively inconsequential, because the moment the attack is initiated, it is also fulfilled and the damage is caused. Alternatively, however, some cyber operations, such as a logic bomb—a piece of code deliberately inserted into a software system that triggers destructive or malicious functions upon certain specified conditions—have a lag time that can make the immediacy analysis more challenging, especially in conjunction with the necessity requirement. Although

35. The United States has clearly stated that it reserves the right to use both cyber and kinetic force, as needed, in response to cyber attacks or imminent cyber attacks. *See* U.S. Department of Defense, Cyberspace Policy Report 4 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

the armed attack may occur at the moment when the logic bomb is inserted into the software, fulfilling the immediacy requirement, to the extent that a State has non-forceful options for "defusing" the logic bomb before it is actually triggered, the lag time would mean that necessity is not present if such alternatives exist.

III. THE LAW OF ARMED CONFLICT

A second category or legal paradigm that applies—in different circumstances—to a State's response to cyber threats or attacks by non-State actors is the law of armed conflict. LOAC, also known as the law of war and international humanitarian law, governs the conduct of both States and individuals during armed conflict. It seeks to minimize suffering in war by protecting persons not participating in hostilities and by restricting the means and methods of warfare.[36] LOAC applies during all situations of armed conflict, with the full panoply of the Geneva Conventions and customary law applicable in international armed conflict and a more limited body of treaty and customary law applicable during non-international armed conflict. The lawfulness of targeting individuals and objects during armed conflict is determined by the principles of distinction, proportionality and precautions. With regard to the cyber arena, questions regarding responses to non-State actors fall into two primary areas: (1) the situation in which the State seeks to respond to the non-State actor in an armed conflict such that LOAC does apply; and (2) the status or nature of the non-State actors for the purposes of analyzing whether and how the State can

36. *See* International Committee of the Red Cross, *What Is International Humanitarian Law?*, ICRC (July 31, 2004), http://www.icrc.org/eng/resources/documents/legal-fact-sheet/humanitarian-law-factsheet.htm. The law of armed conflict is codified primarily in the four Geneva Conventions of August 12, 1949, and their Additional Protocols. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609.

target and/or detain them in the course of that conflict.

A. Does the State vs. Non-State Activity Constitute an Armed Conflict?

LOAC applies only during an armed conflict; thus determining whether the violence between the State and the non-State actor rises to the level of an armed conflict is the essential first analytical step in understanding if the State may respond to cyber threats posed by non-State actors within the paradigm of armed conflict. The 1949 Geneva Conventions endeavor to address all instances of armed conflict[37] and set forth two primary categories of armed conflict that trigger the application of LOAC: international armed conflict and non-international armed conflict. Common Article 2 of the 1949 Geneva Conventions states that the Conventions "shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[38] Common Article 3 of the 1949 Geneva Conventions sets forth minimum provisions applicable "in the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties."[39] Notably, the Geneva Conventions adopted the term "armed conflict" specifically to avoid the technical legal and political pitfalls of the term "war."[40] As such, determination of the existence of an armed conflict does not turn on a formal declaration of war—or even on how the participants characterize the hostilities—but rather on the facts of a given situation.[41]

---

37. COMMENTARY ON GENEVA CONVENTION IV RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 26 (Oscar M. Uhler & Henri Coursier eds., 1958) [hereinafter GC IV COMMENTARY] ("Born on the battlefield, the Red Cross called into being the First Geneva Convention to protect wounded or sick military personnel. Extending its solicitude little by little over other categories of war victims, in logical application of its fundamental principle, it pointed the way, first to the revision of the original convention, and then to the extension of legal protection in turn to prisoners of war and civilians. The same logical process could not fail to lead to the idea of applying the principle in *all* cases of armed conflicts, including those of an internal character.").

38. GCI, GC II, GC III, GC IV art.2, *supra* note 36 [hereinafter Common Article 2].

39. *Id.*, art. 3.

40. GC IV COMMENTARY, *supra* note 37, at 17–25.

41. Common Article 2 of the 1949 Geneva Conventions applies to "all cases of declared war or of any other armed conflict . . . between two or more [States], even if the state of war is not recognized by one of them." Common Article 2, *supra* note 38. *See, e.g.*, Anthony Cullen, *Key Developments Affecting the Scope of Internal Armed Conflict in International*

The International Criminal Tribunal for the former Yugoslavia (ICTY) set forth the modern definition of armed conflict in *Prosecutor v. Tadić*, stating that an armed conflict exists whenever "there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[42] This definition describes both international armed conflict (armed force between States) and non-international armed conflict (protracted armed violence between governments and organized armed groups). In this subsection, the discussion will focus on the legal issues in identifying a non-international armed conflict between a State and non-State actors within the cyber arena. Of course, a State involved in an international armed conflict with another State may well face cyber threats from a non-State actor also participating in the conflict, perhaps acting in coordination with the opposing State, but the questions surrounding how the nature of that non-State actor impacts the identification of an armed conflict and the actual triggering of LOAC would not arise in the same way. As jurisprudence stemming from this definition has developed over the past two decades with regard to non-international armed conflict, two considerations have dominated the discourse, particularly in the decisions of the ICTY and other international tribunals—the intensity of the fighting and the organization of the parties.[43]

Intensity requires an analysis of the seriousness of the fighting in order to determine whether it has passed from riots and other random acts of violence to engagements more akin to regularized military action. There is little doubt that a cyber-based conflict could, at some point, reach a sufficient level of intensity to satisfy this threshold; however, the evidence or

---

Humanitarian Law, 183 MILITARY LAW REVIEW 66, 85 (2005) ("[I]t is worth emphasizing that recognition of the existence of armed conflict is not a matter of state discretion.").

42. Prosecutor v. Tadić, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter *Prosecutor v. Tadić* (Decision on Interlocutory Appeal)].

43. Prosecutor v. Tadić, Case No. IT-94-1-T, Judgment, ¶ 562 (Int'l Crim. Trib. for the former Yugoslavia May 7, 1997) [hereinafter *Prosecutor v. Tadić* (Judgment)]; Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 84 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Prosecutor v. Boskoski & Tarculovski, Case No. IT-04-82-T, Judgment, ¶ 175 (Int'l Crim. Trib. for the former Yugoslavia July 10, 2008). For a counterargument to the increasingly formalized application of these two elements or factors, see Laurie R Blank and Geoffrey S. Corn, *Losing the Forest for the Trees: Syria, Law and the Pragmatics of Conflict Recognition*, 46 VANDERBILT JOURNAL OF TRANSNATIONAL LAW (forthcoming 2013).

analysis of such intensity could differ from the factual information used in a kinetic scenario. Traditionally, analyzing intensity has encompassed a range of specific factors regarding the actual hostilities. For example, the ICTY has considered factors such as the number, duration and intensity of individual confrontations; the types of weapons and other military equipment used; the number of persons and types of forces engaged in the fighting; the geographic and temporal distribution of clashes; the territory that has been captured and held; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zones.[44] The ICTY has also declared that the involvement of the UN Security Council may reflect the intensity of a conflict.[45] The collective nature of the fighting, the State's resort to use of its armed forces, the duration of the conflict, and the frequency of the acts of violence and military operations are all additional factors to take into account as well. Most or all of these considerations are highly relevant in the cyber context as well (with the exception, perhaps, of the capture of territory), but the analysis will rely overwhelmingly on the effects of attacks rather than the types of operations, the engagement of forces or the number of persons involved, because those categories of information are extremely difficult to assess in the cyber arena.

In the scenario of a potential conflict between a State and non-State actors using cyber attacks as the main form of attack, the second factor of organization is of particular interest. Various international tribunals and other courts have looked to a non-State actor's level of organization as one way to distinguish armed conflict from unorganized violence and riots. Rigid adherence to specific measures or types of organization have the potential to undermine the effectiveness of LOAC by hindering its application to situations that otherwise seem to obviously fall within the notion of an armed conflict.[46] Nonetheless, whether one takes a more formalized approach to the definition of armed conflict, relying heavily on the intensity/organization factors, or a more totality-of-the-circumstances approach, some notion of an opposing party fighting against the State is essential to characterizing a situation as an armed conflict for the application of LOAC. Here the cyber arena poses potentially unique challenges, especially in the

44. Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); *Prosecutor v. Limaj*, *supra* note 43, ¶¶ 135–43; *Prosecutor v. Tadić* (Judgment), *supra* note 43, ¶¶ 564–65.

45. *Prosecutor v. Haradinaj*, *supra* note 44, ¶ 49.

46. *See* Blank and Corn, *supra* note 43.

context of non-State actors launching attacks on the State.

Factors traditionally considered as important in determining whether a group is sufficiently organized to be a party to an armed conflict include a hierarchical structure, territorial control and administration, the ability to recruit and train combatants, the ability to launch operations using military tactics and the ability to enter peace or ceasefire agreements.[47] The International Committee of the Red Cross (ICRC) has also highlighted the non-State actor's authority to launch attacks bringing together different units and the existence or promulgation of internal rules.[48] To the extent that a non-State armed group is engaged in a struggle against government forces in which cyber operations form only one tool in that struggle, the analysis will be similar to that in other situations, such as those highlighted in the ICTY's jurisprudence in which it, for example, examined the nature of the Kosovo Liberation Army in determining whether it constituted an organized armed group such that the violence in Kosovo was an armed conflict. The more interesting question and the one directly relevant to the instant analysis, however, is how to determine the existence of a non-international armed conflict when the non-State actors engage with the government solely in the cyber realm. Can a seemingly "virtual conflict" be an armed conflict that triggers LOAC?

At one end of the spectrum would be a group that is organized with some type of command structure, a decision making and operational planning process, and the ability to launch operations. In essence, the type of weapon used—cyber—would be the main distinction between this type of group and an organized armed group using kinetic force and there would be little question that such a group is sufficiently organized to meet the criterion of organization to be a party to an armed conflict. Much more likely, however, is that cyber attacks by non-State actors against a government would be carried out by independent actors, disparate actors sharing similar goals or even loosely affiliated groups of hackers or other actors. "Autonomous actors who are simply all targeting a State, perhaps in response to a broad call to do so from one or more sources," but without any formal di-

47. *See Prosecutor v. Limaj*, *supra* note 43, ¶¶ 95–109; Prosecutor v. Lukić, Case No. IT-98-32/1-T, Judgment, ¶ 884 (Int'l Crim. Trib. for the former Yugoslavia July 20, 2009); *Prosecutor v. Haradinaj*, *supra* note 44, ¶ 60.

48. Sylvain Vité, *Typology of Armed Conflicts in International Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 77 (2009).

rection or structure, "cannot be deemed to be organized."[49] As the *Commentary* to the Additional Protocols explains, "individuals operating in isolation" generally do not fit within the understanding of "organized."[50]

The nature of the virtual world, in which members of groups—even ones with a high degree of organization and shared purpose—have no face-to-face contact or connection, compounds the challenges of identifying sufficient organization to meet the definition of armed conflict. For example, during the conflict between Georgia and Russia in the summer of 2008, numerous cyber attacks were launched against Georgia. Most of these attacks were initiated using information from a website that provided cyber tools and lists of Georgian government websites and cyber targets. The attacks were not coordinated with regard to timing, target and effect, or in any other aspect. Based on existing analyses of the *Tadić* definition of armed conflict and the requisite components of the factor of organization, something more than this type of merely collective action would be needed in the solely cyber realm. It has been argued that the determination of whether a group acting for a shared purpose "meets the organization criterion should depend on such context-specific factors as the existence of a formal or informal leadership entity directing the group's activities in a general sense, identifying potential targets and maintaining an inventory of effective hacker tools."[51]

The scenario of a cyber-only engagement between non-State actors and a State that is of sufficient intensity to merit consideration as an armed conflict may seem far-fetched at this point, but it is possible and if it were to occur, it would raise questions as to whether LOAC applies. Just as the scattered nature of the opposition to government forces in a kinetic environment could forestall the recognition of an armed conflict—as the international community argued for many months with regard to the conflict in Syria[52]—such arguments would have significantly greater force in a cyber-

---

49. Michael N. Schmitt, *Cyber Operations and the* Jus in Bello: *Key Issues*, 41 ISRAEL YEARBOOK ON HUMAN RIGHTS 113, 124–25 (2011).

50. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1672 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

51. Schmitt, *supra* note 49, at 125. Although Schmitt's analysis focuses on the identification of an organized armed group for the purposes of distinguishing members of that group from civilians in the context of a direct participation in hostilities analysis, it is equally useful in the present context of analyzing the extent of a group's organization for the purposes of finding an armed conflict that triggers the application of LOAC.

52. *See* Blank and Corn, *supra* note 43.

only engagement. It is nonetheless important to understand how the law delineates between non-conflict and armed conflict, precisely because the parameters of the government response to the non-State actors engaged in cyber operations change dramatically between the law of peacetime and the law of wartime, as the following subsection details.

B. Responding to Non-State Actors in the Course of Armed Conflict

Within the context of an armed conflict—whether mixed kinetic and cyber or perhaps solely cyber, as in the less likely scenario alluded to above—the essential issues will be identifying who or what can be targeted and who can be detained. Even more than in "normal" or kinetic conflict, in the cyber arena, intelligence information is critically important, particularly because of the heightened challenges of attribution in the cyber context. Indeed, anonymity is one of the greatest advantages that cyber warfare offers to both States and non-State actors. With regard to targeting, attribution (for both persons and objects) plays a central role in the identification of targets—mandated by the principle of distinction—but also in operationalizing the obligations of proportionality and precautions. Moreover, each of these three fundamental principles has an even more acute protective role to play in a non-international armed conflict, where the lines between fighter and civilian are often extremely blurred.

1. Identifying and Classifying Non-State Actors in Cyber Conflict

The principle of distinction, one of the "cardinal principles" of LOAC,[53] requires that any party to a conflict distinguish between those who are fighting and those who are not and direct attacks solely at the former. Similarly, parties must distinguish between civilian objects and military objects and target only the latter. Article 48 of Additional Protocol I sets forth the basic rule: "[I]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their op-

53. *Nuclear Weapons*, *supra* note 33, ¶ 78 (Higgins, J., dissenting on unrelated grounds) (declaring that distinction and the prohibition on unnecessary suffering are the two cardinal principles of international humanitarian law).

erations only against military objectives.[54]

Distinction lies at the core of LOAC's seminal goal of protecting innocent civilians and persons who are *hors de combat*. The obligation to distinguish is part of the customary international law of both international and non-international armed conflicts, as the ICTY held in the *Tadić* case.[55] The purpose of distinction—to protect civilians—is emphasized in Article 51 of Additional Protocol I, which states that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack."[56] Furthermore, Article 85 of Protocol I declares that nearly all violations of distinction constitute grave breaches of the Protocol.[57] The Rome Statute similarly criminalizes attacks on civilians and indiscriminate attacks.[58]

Distinction requires identification of lawful targets as a prerequisite to the use of force in armed conflict. A lawful attack must be directed at a legitimate target—a combatant, member of an organized armed group, civilian directly participating in hostilities or military objective. In international armed conflicts, all members of the State's regular armed forces are combatants and can be identified by the uniform they wear, among other characteristics. Other persons falling within the category of combatant include members of volunteer militias who meet four requirements: wearing a distinctive emblem, carrying arms openly, operating under responsible com-

---

54. AP I, *supra* note 36, art. 48. Article 48 is considered customary international law. *See* 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3–8 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter CIHL].

55. *Prosecutor v. Tadić* (Decision on Interlocutory Appeal), *supra* note 43, ¶ 110 ("Bearing in mind the need for measures to ensure the better protection of human rights in armed conflicts of all types, [the General Assembly] Affirms the following basic principles for the protection of civilian populations in armed conflicts, without prejudice to their future elaboration within the framework of progressive development of the international law of armed conflict: . . . [i]n the conduct of military operations during armed conflicts, a distinction must be made at all times between persons actively taking part in the hostilities and civilian populations." (quoting G.A. Res. 2675, U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028 (Dec. 9, 1970). *See also Nuclear Weapons*, *supra* note 33, ¶ 79 (distinction is one of the "intransgressible principles of international customary law"); CIHL, *supra* note 54, at 3–8; Abella v. Argentina, Case 11.137, Inter-Am. C.H.R., Report No. 55/97, OEA/Ser.L/V/II.95, doc. 7 rev. ¶¶ 177–178 (1997).

56. AP I, *supra* note 36, art. 51(2).

57. *Id.*, art. 85.

58. *See* Rome Statute of the International Criminal Court arts. 8(2)(b)(i), 8(2)(b)(ii), 8(2)(b)(iv), 8(2)(b)(v), 8(2)(b)(vi), 8(2)(e)(i), 8(2)(e)(ii), 8(2)(e)(iv), July 17, 1998, 2187 U.N.T.S. 90, *available at* http://untreaty.un.org/cod/icc/statute/english/rome_statute(e).pdf.

mand and abiding by the law of armed conflict.[59] Members of the regular armed forces of a government not recognized by the opposing party and civilians participating in a *levée en masse* also qualify as combatants in international armed conflict.[60] Combatants can be attacked at all times and enjoy no immunity from attack, except when they are *hors de combat* due to sickness, wounds or capture. To the extent that a State is responding to cyber threats or attacks by non-State actors in an international armed conflict, the first question will be whether the non-State actor falls within one of these combatant categories. Although unlikely, if they do, the non-State actors will be targetable at all times on the basis of their status as combatants. Assuming they do not, then the non-State actors remain civilians and retain their immunity from attack except at such times as they directly participate in hostilities. Each of these considerations will be addressed below. For each category the analysis with regard to non-international armed conflict applies in international armed conflict as well.

In non-international armed conflicts, which are most often between a State and a non-State entity, but can be between or among multiple non-State groups, there is no combatant status; thus operationalizing distinction relies on alternative means of distinguishing those who are fighting from those who are not. A significant question is therefore whether members of opposition groups are simply civilians fighting against the government or constitute an organized force distinct from the civilian population.[61] If they are civilians, then they are immune from attack except when directly participating in hostilities, like all other civilians. If they are members of an organized armed force, then they are targetable at all times, regardless of whether they are engaged in hostilities at the time.[62] In general, the term

59. GC III, *supra* note 36, art. 4(A)(2).

60. *Id.*, arts. 4(A)(3), 4(A)(6).

61. For a comprehensive discussion of the status of persons fighting against the government in a non-international armed conflict, see Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, *in* NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 119 (Kenneth Watkin & Andrew J. Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies).

62. *See* JIMMY GURULÉ & GEOFFREY S. CORN, PRINCIPLES OF COUNTER-TERRORISM LAW 70–76 (2011) (discussing the rules governing targeting of enemy forces in international and non-international armed conflict and noting that (1) "a member of an enemy force . . . is presumed hostile and therefore presumptively subject to attack" in international armed conflict and (2) "subjecting members of organized belligerent groups to status based targeting pursuant to the LOAC as opposed to civilians who periodically lose their protection from attack seems both logical and consistent with the practice of states engaged in non-international armed conflicts"); NILS MELZER, INTERNATIONAL COM-

"organized armed group"—used to describe the non-State party to a conflict—refers specifically to the military wing of a non-State actor, essentially the functional equivalent of the government armed forces. Organized armed groups "recruit their members primarily from the civilian population but develop a sufficient degree of military organization to conduct hostilities on behalf of a party to the conflict, albeit not always with the same means, intensity and level of sophistication as State armed forces."[63] A commonly used, but still contentious, method for identifying members of organized armed groups is the notion of continuous combatant function, introduced in the ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities*. As the *Guidance* explains, "membership [in an organized armed group] must depend on whether the continuous function assumed by an individual corresponds to that collectively exercised by the group as a whole, namely the conduct of hostilities on behalf of a non-State party to the conflict."[64] Although there remains extensive debate regarding the concept of continuous combat function and the identification of members of an organized armed group, such debate is outside the scope of this article. Rather, for the purposes of the instant analysis, it is sufficient to focus on the fundamental distinction that is recognized between members of an organized armed group and civilians.

The cyber-specific issues in this area are quite similar to those raised in the earlier discussion regarding the nature of organization for purposes of classifying an armed conflict. If individuals who engage in cyber attacks against the State are part of an organized armed group, they will be targetable at all times. The challenge lies in identifying an organized group that operates solely in the cyber realm and, as a second step, in identifying the members of that group so as to make targeting decisions appropriately.

A second category of individuals who can be targeted lawfully under LOAC is civilians who take direct part in hostilities. Such persons are legitimate targets of attack during and for such time as they engage directly in hostilities.[65] In certain limited circumstances, therefore, civilians may be

---

MITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 16–17 (2009), *reprinted in* 90 INTERNATIONAL REVIEW OF THE RED CROSS 991, 996 (2008), *available at* http://www.icrc. org/eng/assets/files/other/icrc-002-0990.pdf (stating that organized armed groups are targetable based on status in non-international armed conflict) [hereinafter INTERPRETIVE GUIDANCE].

63. INTERPRETIVE GUIDANCE*, supra* note 62, at 32.

64. *Id.* at 33.

65. AP I, *supra* note 36, art. 51(3).

directly and intentionally targeted during hostilities. Thus, "[t]he principle of distinction acknowledges the military necessity prong of [the law's] balancing act by suspending the protection to which civilians are entitled when they become intricately involved in a conflict."[66] In recent years, courts and commentators have struggled to define the concept of direct participation in hostilities and develop parameters for understanding when civilians—as the term is traditionally used—become legitimate targets by reason of such participation.[67] A detailed analysis of direct participation is outside the scope of this article; it is sufficient to define direct participation in hostilities as acts intended to harm the enemy or the civilian population in a direct or immediate manner, therefore making the actor a legitimate target of attack for the purposes of distinction within LOAC. The analysis here will focus specifically on identifying direct participation in the cyber arena.

Some examples of cyber acts that could constitute direct participation in hostilities include writing and executing malicious code, launching distributed denial of service attacks, providing malware or other cyber tools to a party to the conflict, or other forms of cyber attack. More complicated questions involve the status of persons who engage in cyber operations that do not qualify as cyber attacks but contribute directly to cyber operations and cyber attacks, such as hacking into an enemy computer to gather intelligence to be used in the launching of an attack or planting a worm in software that breaks down defenses, thus enabling a subsequent attack to

---

66. Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 5, 12 (2010).

67. *See, e.g.*, HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006 (2) PD 459 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS 373, *available at* http://elyon1.court.gov.il/Files_ENG/02/690/007/a34/02007690.a34.pdf [hereinafter *Targeted Killings*]; Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Judgment, ¶ 616 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999). *See generally* CIHL *supra* note 55, at 2–9; Jason Callen, *Unlawful Combatants and the Geneva Conventions*, 44 VIRGINIA JOURNAL OF INTERNATIONAL LAW 1025 (2004); Derek Jinks, *Protective Parity and the Laws of War*, 79 NOTRE DAME LAW REVIEW 1493, 1495–1501 (2004); Jann K. Kleffner, *From "Belligerents" to "Fighters" and Civilians Directly Participating in Hostilities—On The Principle of Distinction in Non-International Armed Conflicts One Hundred Years After the Second Hague Peace Conference*, 54 NETHERLANDS INTERNATIONAL LAW REVIEW 315 (2007); INTERPRETIVE GUIDANCE, *supra* note 63; W. Hays Parks, *Air War and the Law of War*, 32 AIR FORCE LAW REVIEW 1 (1990); Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHICAGO JOURNAL OF INTERNATIONAL LAW 519, 522–36 (2005); Kenneth W. Watkin, *Combatants, Unprivileged Belligerents and Conflict in the 21st Century*, 1 ISRAEL DEFENSE FORCES LAW REVIEW 69 (2003).

be successful.[68] In any of these or other situations, identifying direct participation requires that the act in question cause harm directly to the opposing side or to civilians and that it have a nexus to the armed conflict.[69]

Some of the already challenging conceptual issues in applying direct participation in hostilities in kinetic operations become even thornier in the framework of cyber operations. Beyond the identification of the types of acts or contributions that fit within the notion of direct participation, the "for such time as" component of direct participation proves to be especially complex. It is generally accepted that acts preparatory to or returning from a deployment are considered to be part of the act that constitutes direct participation in hostilities.[70] Here, an initial question must be how to determine which acts constitute the actual attack, which are considered preparatory to execution or deployment, and which are too attenuated to fit within the paradigm. The malware, worm or other trigger of a cyber attack will often be inserted into the relevant software, server or network well in advance of the actual time of the attack or eventual consequences, which naturally raises the question of when the individual launching the attack is directly participating in hostilities. Is it only when designing and inserting the malware? When the attack is actually launched, as well for the duration of the attack? And in the instantaneous world of virtual communications and cyber operations, identifying the conduct that should be considered to be preparatory to or returning from execution or deployment simply may not be relevant or possible. As a result, the same questions of a revolving door[71]—the farmer by day, fighter by night example—arise in cyber as in other types of operations, but perhaps with greater urgency and even less discernibility.

---

68. *See* Yoram Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 261, 263 (2012) (stating that the following do not qualify as cyber attacks because they do not produce violent effects: hacking into an enemy computer for intelligence-gathering purposes, breaking through a computer's firewall, planting a worm in digital software, extracting secret data, gaining control over codes and disrupting communications).

69. *See, e.g.*, INTERPRETIVE GUIDANCE*, supra* note 62, at 46 (three key components of direct participation are the threshold of harm, direct causation and belligerent nexus). *See also* David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 279 (2012) (providing a chart analyzing ten different types of cyber acts within the framework of threshold of harm, direct causation and belligerent nexus).

70. INTERPRETIVE GUIDANCE*, supra* note 62, at 65.

71. *See Targeted Killings*, *supra* note 67.

Finally, the requirement that there be a belligerent nexus, a connection between the relevant act and the ongoing armed conflict, can certainly pose particular challenges in the cyber arena, where it can be difficult in some situations to distinguish hacking, cyber crime and cyber espionage from more conflict-related cyber acts. As a result, States considering responses to cyber activity by non-State actors will need to rely on extensive cooperation between the law enforcement, intelligence and military communities in order to ensure an effective and lawful response to cyber acts and cyber threats.

These distinctions between individuals—whether members of organized armed groups, civilians directly participating in hostilities or innocent civilians—are relevant not only during combat operations, when one side has to make determinations about who and what is targetable, who can be detained, and who and what must be protected. They are also significant—indeed foundational—considerations in any post-conflict accountability process. For example, the crime of attacking civilians depends, at first, on the identification of the victims as civilians who are entitled to immunity from attack (i.e., they are not directly participating in hostilities at the time of the attack). In a prosecution for attacks on civilians during non-international armed conflict, a defendant is likely to argue that the victims were not civilians but rather were members of the opposing forces. As noted above with regard to responses to non-State actors during the course of conflict, the necessary linkage between the cyber operations of the individuals who were attacked and the armed conflict will be the central issue in the accountability paradigm as well. Crimes and criminal activity persist and often flourish during armed conflict, but that does not mean that all crimes and all criminals should be prosecuted within a LOAC framework. Rather, there must be a nexus between the act and the armed conflict in order for international criminal accountability to attach.[72] Here, the ability to distinguish between cyber crime and other "non-war" cyber activities, to identify which cyber activities are linked to an ongoing conflict and which are simply opportunistic criminal activity, is a prerequisite to any accountability efforts after the conflict.

72. Prosecutor v. Kunarac, Case No. IT-96-23/1-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia Feb. 22, 2001).

2. Proportionality and Precautions

Legal analysis does not end with identification of a legitimate target. Rather, the attacking party must then assess whether the attack meets the requirements of the principle of proportionality and take other necessary precautions to comply with LOAC's mandates. Detailed specifically in Additional Protocol I, these obligations apply as a matter of customary international law in all conflicts, whether international or non-international. The primary issue with regard to State responses to cyber attacks or threats from non-State actors is, as explored in greater detail above, the challenge of identifying which individuals and objects are legitimate targets for attack and which are civilian in nature and protected from attack under LOAC. This subsection will, therefore, simply provide a brief explanation of the fundamental obligations of proportionality and precautions that apply to any cyber attack launched against non-State actors in the course of an armed conflict, without delving deeply into the broader issues relevant to proportionality and precautions in the cyber context that would arise across the spectrum of conflict.[73] One example is the cascading effects that cyber attacks can have and how to analyze such effects for the purposes of proportionality.

The principle of proportionality requires that parties refrain from attacks in which the expected civilian casualties will be excessive in relation to the anticipated military advantage gained. Additional Protocol I contains three separate statements of the principle of proportionality. The first appears in Article 51, which sets forth the basic parameters of the obligation to protect civilians and the civilian population, and prohibits any "attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[74] This language demonstrates that Additional Protocol I contemplates incidental civilian casualties. It appears again in Articles 57(2)(a)(iii)[75]

73. For an analysis of precautions and proportionality in the cyber context, see Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INTERNATIONAL LAW STUDIES 198 (2013).

74. AP I, *supra* note 36, art. 51(5)(b).

75. *Id.*, art. 57(2)(a)(iii) ("With respect to attacks, the following precautions shall be taken: [t]hose who plan or decide upon an attack shall . . . [r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . .").

and 57(2)(b),[76] which refer specifically to precautions in attack. Proportionality is not a mathematical concept, but rather a guideline to help ensure that military commanders weigh the consequences of a particular attack and refrain from launching attacks that will cause excessive civilian deaths or damage to civilian property.

LOAC also mandates that all parties take certain precautionary measures to protect civilians. In many ways, the identification of military objectives and the proportionality considerations are, of course, precautions. But the obligations of the parties to a conflict to take precautionary measures go beyond that. Beginning at the broadest level, Article 57(1) of Additional Protocol I states, "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[77] This provision is a direct outgrowth of and supplement to the Basic Rule in Article 48, which mandates that all parties distinguish between combatants and civilians and between military objects and civilian objects. The practical provisions forming the major portion of Article 57 discuss precautions to be taken specifically when launching an attack. First, parties must do everything feasible to ensure that targets are military objectives. Doing so helps to protect civilians by limiting attacks to military targets, thus directly implementing the principle of distinction. Second, they must choose the means and methods of attack with the aim of minimizing incidental civilian losses and damage. For example, during the 1991 Persian Gulf War, "pilots were advised to attack bridges in urban areas along a longitudinal axis. This measure was taken so that bombs that missed their targets—because they were dropped either too early or too late—would hopefully fall in the river and not on civilian housing."[78] Another common method of taking precautions is to launch attacks on particular targets at night when the civilian population is not on the streets or at work, thus minimizing potential casualties. In addition, when choosing between two

76. *Id.*, art. 57(2)(b) ("An attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . .").

77. *Id.*, art. 57(1).

78. Jean-François Quéguiner, *Precautions Under the Law Governing the Conduct of Hostilities*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 793, 801 (2006) (noting that this angle of attack "also means that damage would tend to be in the middle of the bridge and thus easier to repair") (citing Michael W. Lewis, *The Law of Aerial Bombardment in the 1991 Gulf War*, 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 481 (2003)).

possible attacks offering similar military advantage, parties must choose the objective that offers the least likely harm to civilians and civilian objects. Finally, Article 57(2)(c) requires attacking parties to issue an effective advance warning "of attacks which may affect the civilian population, unless circumstances do not permit."[79]

The issues of attribution and distinction discussed above are equally relevant with regard to proportionality and precautions. Proportionality's obligations only attach when some civilian casualties, injury or damage are expected to occur; making such determinations relies first on the ability to determine that some of the potential victims of the attack will be civilians. Similarly, the various precautionary obligations demand an ability to distinguish between military and civilian objects and to identify where civilians are located, if warnings are needed, and how to provide such warnings and other protections against the effects of attacks. In the course of an armed conflict with a non-State armed group—whether a more traditional armed group or one that fights primarily with cyber weapons—the State must develop and use the capacity to identify and differentiate between civilian and military persons and objects, not only for the purposes of identifying whom it is fighting against but also for the purposes of protecting those who are uninvolved in the conflict and merit protection under LOAC.

IV. RHETORIC AND ITS CONSEQUENCES IN OPERATIONS AGAINST NON-STATE ACTORS

In considering the parameters of State responses to cyber threats from non-State actors, it is important to recognize the role that rhetoric does and can play in this arena. Terms such as "cyber war," "cyber warfare" and "cyber attack" are used to describe a broad array of activities, many of which fall outside the scope of the types of attacks discussed here, the types of attacks that trigger the *jus ad bellum* or attacks as that term is used within LOAC. For example, an early definition of cyber warfare, but one still in regular use, is "any operation that disrupts, denies, degrades, or destroys information resident in computers or computer networks."[80] In another study, the authors split cyber warfare into five general varieties, ranging from the mildest to the most severe: (1) web vandalism, (2) disinformation campaigns, (3) gathering secret data, (4) disruption in the

79. AP I, *supra* note 36, art. 57(2)(c).

80. WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 132 (1999).

field and (5) attacks on critical national infrastructure.[81] The use of terms that sound like "war" but are in fact much broader in scope than the corresponding legal terms and definitions can have significant consequences for the application of the law, the execution of operations and the protection of persons and property.

Counterterrorism policy over the past decade offers a prime example of the impact rhetoric can have on the development and implementation of the law. The rhetoric of the "war on terror" facilitated and encouraged the growth of authority without the corresponding obligation in many cases. For example, the drone campaign in Pakistan, indefinite detention, prosecution of crimes such as conspiracy or material support for terrorism in military commissions and other practices have raised significant questions about the application of domestic and international law to counterterrorism operations, the long-term impact on executive authority and the use of national security as a "trump card" in the face of legal obstacles or challenges. In addition, layering rhetoric on top of the law has affected the application and implementation of key bodies of law, such as human rights law, LOAC and various domestic legal regimes relevant to national security and counterterrorism.[82] Over the course of several years, the mix of counterterrorism operations and military operations, and a rhetoric of war that subsumed both, helped lead to minimized rights and magnified executive powers.

Just as the rhetoric of war subsumed a wide variety of counterterrorism measures within the concept of a "war on terror" and ultimately had a profound effect on both law and policy with respect to counterterrorism and war, so the potential for similar consequences in the cyber arena exists as well. Cyber activities can span a continuum of "bad activity" from cyber crime to cyber espionage to cyber terrorism an all the way to cyber attacks and cyber war. Not all of these acts fit within the paradigm of international law governing the use of force or the LOAC regime, as detailed earlier in this article. As a result, it is essential to differentiate between actors with "war" intentions and those with malicious or criminal intentions, especially when assessing the appropriate response to non-State actors engaged in

---

81. *See* Center for the Study of Technology and Society, *Special Focus: Cyberwarfare,* http://web.archive.org/web/20061205020720/tecsoc.org/natsec/focuscyberwar.htm (2001).

82. *See generally* Laurie R. Blank, *The Consequences of a "War" Paradigm for Counterterrorism: What Impact on Basic Rights and Values?*, 46 GEORGIA LAW REVIEW 719 (2012).

some type of damaging cyber conduct.[83] Understanding the impact of certain rhetorical choices is equally important. For example, the term "cyber attack" is regularly used in the mass media to denote an extremely wide range of cyber conduct, much of which falls well below the threshold of an "armed attack" as understood in the *jus ad bellum* or an attack as defined in LOAC for purposes of triggering the obligations of distinction, proportionality and precautions. Rhetoric that uses a terminology of war, like "cyber war" or "cyber attack," can create situations in which a State has fewer obstacles to an aggressive response to a non-State actor's cyber threats or cyber conduct, stretching or overstepping the relevant legal boundaries. In this way, such rhetoric poses a serious risk of elevating or escalating an apparently hostile action to the status of war or conflict when, in the absence of such rhetoric, it would be more appropriately handled or countered within the criminal system or other non-forceful paradigm.

The interplay between law and rhetoric thus forms an important backdrop to the analysis of the international legal norms that govern how a State can respond to cyber threats from non-State actors. Rhetoric that opens the door to overly broad responses necessitates an understanding of the relevant legal paradigms, the boundaries between them and the fundamental principles that guide their application. Use of terms like "war" and "attack" for a much wider array of activities also facilitates a blurring of the lines between relevant and applicable legal frameworks, which can have a detrimental effect on both individual rights and the development of the law. With regard to cyber threats and cyber attacks, both the *jus ad bellum* and LOAC help shape the parameters of lawful and effective action in response to non-State actors, not only by guiding the appropriate conduct when force may lawfully be used or during armed conflict, but also by delineating the dividing line between crime and war and between self-defense and law enforcement.

---

83. *See, e.g.*, Nils Melzer, *Cyber Operations and* Jus in Bello, DISARMAMENT FORUM, no. 4, 2011, at 3, *available at* http://www.unidir.org/pdf/articles/pdf-art3164.pdf ("Applied to the more specific context of cyber operations, this means that the use of the terms 'cyberwar,' 'cyberwarfare,' 'cyberhostilities,' and 'cyberconflict' should be restricted to armed conflicts within the meaning of [international humanitarian law]. Indeed, security threats emanating from cyberspace that do not reach the threshold of armed conflict can be described as 'cybercrime,' 'cyber operations,' 'cyberpolicing' or, where appropriate, as 'cyberterrorism' or 'cyberpiracy,' but should not be referred to with terminology inviting doubt and uncertainty as to the applicability of the law of armed conflict.").