CYBERTERRORISTS: THE IDENTIFICATION AND CLASSIFICATION OF NON-STATE ACTORS WHO ENGAGE IN CYBER-HOSTILITIES

MAJOR ANDREA C. GOODE*

The very technologies that empower us to lead and create also empower those who would disrupt and destroy.[1]

I. Introduction

Sometime in the near future, the 31st Marine Expeditionary Unit (31st MEU), onboard the United States Ship (USS) *Bonhomme Richard*, pulls into port in Singapore, Malaysia. That same day, there is a devastating terrorist attack in Subic Bay, Philippines, which results in an unknown number of deaths and casualties. The 31st MEU receives orders to deliver critical disaster relief supplies to the victims of the attack and provide a presence within Subic Bay to deter and defeat additional attacks. Meanwhile, a sailor from the USS *Bonhomme Richard*, contrary to the directives of the numerous security briefings that he received before departing the ship, purchases an Universal Serial Bus (USB) flash drive from a port vendor, which contains thirty pirated new release movies. Eager to watch the latest Michael Bay action film, he plugs the thumb drive into his government computer as soon as he returns to the ship. Unbeknownst to him, as the action on the screen unfolds, action of a more sinister sort begins as a worm infiltrates the

* Judge Advocate, U.S. Marine Corps. Presently assigned as the Staff Judge Advocate, U.S. Marine Corps Forces, Europe and Africa; LL.M., 2014, The Judge Advocate General's School, U.S. Army, Charlottesville, Virginia; J.D., 2003, St. Mary's University School of Law, San Antonio, Texas; B.A., 2000, The College of Charleston, Charleston, South Carolina. Previous assignments include Legal Services Support Section West, Camp Pendleton California, 2010–2013 (Complex Trial Team Prosecutor, 2012–2013; Military Justice Officer, 2011–2012; Senior Trial Counsel, 2010–2011); Trial Counsel, Regional Legal Services Office Southwest, Pensacola Detachment, 2008–2010; Legal Services Support Section West, Camp Pendleton California, 2006–2008 (Defense Counsel, 2007–2008; Trial Counsel, 2006–2007); Operational Law Attorney, Multinational Force Iraq, Baghdad, Iraq, 2005–2006. Member of the bar of California. This article was submitted in partial completion of the Master of Laws requirements of the 62d Judge Advocate Officer Graduate Course.

[1] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY (May 2010) [hereinafter 2010 NATIONAL SECURITY STRATEGY], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

onboard computer systems. The worm then does exactly what it was designed to do: it infiltrates the ship's navigation system and places the radar that controls the navigation system under the complete control of a computer hacker who goes by the alias LulzKhat. As a result, the ship is unable to navigate into Subic Bay's narrow harbor and the 31st MEU is unable to complete its mission.

This hypothetical scenario is not beyond the realm of possibility.[2] The use of cyber capabilities to impact military operations has been increasingly and vigorously addressed at the national level within the last five years. Notable examples include: the establishment of the National Cybersecurity and Communications Integration Center in 2008;[3] the publication of the Cyberspace Policy Review in 2009;[4] the appointment of an Executive Branch Cybersecurity Coordinator that same year;[5] and the creation of U.S. Cyber Command in 2010.[6] In 2011, the White House issued the United States' first International Strategy for Cyberspace, which outlines national strategy for operating in cyberspace using diplomatic, informational, military, and economic means.[7] While national initiatives have risen to the challenge of combating a cyber

---

[2] *See, e.g.*, *USB Memory Sticks and Worms*, UNIV. OF CAMBRIDGE, http://www.ucs.cam.ac.uk/support/windows-support/winsupuser/usbinfections (last visited Feb. 4, 2014); Elliot Bentley, *Tomcat Worm Puts Servers Under Attacker's Remote Control*, JAX MAG. (Nov. 21, 2013), http://jaxenter.com/tomcat-worm-puts-servers-under-attacker-s-remote-control-48983.html.

[3] *The National Cybersecurity and Communications Integration Center*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/about-national-cybersecurity-communications-integration-center (last visited Feb. 12, 2014) (established to protect United States' infrastructure and agency networks from cyber threats).

[4] THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[5] *The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Feb. 12, 2014).

[6] *About Us*, U.S. CYBER COMMAND, https://www.cybercom.mil/default.aspx (last visited Jan. 31, 2014); *see also* 2010 NATIONAL SECURITY STRATEGY, *supra* note 1 (The first National Security Strategy to effectively address the ongoing threat that cyber activities pose to national security).

[7] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (May 2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

attack, international law has not—in large part due to the untraditional nature of cyber warfare.[8]

Cyber war is one of the many types of contemporary conflicts that resist traditional classification. Largely gone are the days of interstate conflicts in which one State's uniformed force confronts another State's uniformed force, while the civilian population remains, in large-part, hidden within shuttered houses until the hostilities are over. The emergence of high-technology warfare—to include cyber war—has changed the battlefield. New technologies have created opportunities for civilians to participate in hostilities at a time when the line between civilians and combatants is increasingly blurred.[9]

The civilianization of armed conflict is further accentuated by the growing rise and potential of stateless groups—such as the Islamic State of Iraq and the Levant, or ISIL—to engage in both inter- and intra-state armed conflict with little regard for geographical borders.[10] In such conflicts, the battlefield encompasses more than a town or valley; terrorism is a global campaign in information operations, where an attack committed in one place may be with the intent to spread fear on a global level.[11] The internet and other cyber assets are effective weapons in this campaign; they can be used to distribute subversive propaganda and disinformation, publicize attacks, and recruit.

To put it simply, computers can be, and are, used for more than information operations. Just as in the opening hypothetical, malware can be created and deployed as a weapon to damage an enemy computer or computer system, disrupt an enemy's communications capabilities, or even disable critical infrastructure. Despite this significant (and growing) potential, as well as the ubiquitous nature of the "weapon," what remains uncertain is the question of how we can respond to such attacks under the law of armed conflict (LOAC).

---

[8] *See, e.g.*, *id.* at 9 ("[The increases in cyber activity] have not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace.").

[9] Andrea Wenger & Simon J. A. Mason, *The Civilianization of Armed Conflict: Trends and Implications*, 90 INT'L REV. OF THE RED CROSS 872, 838 (Dec. 2008).

[10] *Id*. at 847; *see also* Victor D. Cha, *Globalization and the Study of International Security*, 37 J. OF PEACE RES. 3, 391–403 (2000).

[11] IVAN ARREGUIN-TOFT, HOW THE WEAK WIN WARS: A THEORY OF ASYMMETRIC CONFLICT (2005).

The recent publication of the *Tallinn Manual on International Law Applicable to Cyber Warfare* (*Tallinn Manual*) provides some guidance on this issue.[12] However, many questions remain unanswered or unexplored.[13] One particular example is the question of how to identify and classify non-state hostile cyber actors, such as the fictional LulzKhat so that they can be targeted within the boundaries of international law.

This article defines cyberterrorists as non-state actors who use cyber assets to directly participate in hostilities in support of terrorist organizations, such as al-Qaeda, the Taliban, and associated forces, to include ISIL; suggests that these individuals should be classified as unlawful combatants; and concludes that these individuals can be targeted or captured and detained without receiving the rights and privileges that are afforded lawful combatants.

This article begins with a discussion of the history and concept of direct participation in hostilities. It then analyzes how this concept has been interpreted generally and discusses the applicability of those interpretations to cyber activities. Using that discussion as a foundation, this article addresses the classification of identified hostile cyber actors, or cyberterrorists, under LOAC and argues that these individuals should appropriately be classified as unlawful combatants. It concludes with a brief discussion of legally viable actions available to our armed forces when cyberterrorists are identified.

Ultimately, it is the hope of the author to offer commanders answers to the following three questions: (1) What is a cyberterrorist (as opposed to a cybercriminal)?; (2) Do I need to treat him or her as a civilian or as an unlawful combatant?; and (3) What may I lawfully do to/with an identified cyberterrorist?

---

[12] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL], *available at* https://ccdcoe.org/tallinn-manual.html .

[13] *See e.g.*, Michael N. Schmitt, *Cyberspace and International Law: The Penumbral Mist of Uncertainty*, 126 HARV. L. REV. F. 176 (2013), *available at* http://www.harvard lawreview.org/issues/126/march13/forum_1000.php (addressing what Dr. Michael Schmitt, primary author and editor of the *Tallinn Manual*, has termed the "penumbral mist" that surrounds the applicability of international law to cyber war).

II. The Identification of Non-State Hostile Cyber Actors

A. Summary of the History and Concept of Direct Participation in Hostilities

The primary aim of International Humanitarian Law (IHL) is to protect the victims of armed conflict and regulate the conduct of parties to an armed conflict. A pillar of IHL is the principle of distinction, the requirement that military attacks should be directed at combatants and military targets, not civilians or civilian property.[14] In turn, whether a person is a "civilian" turns, in part, on whether that person participated directly in hostilities.

The concept of "direct participation in hostilities" was originally derived from the following language in Common Article 3 of Geneva Conventions I through IV:

> Persons taking *no active part in the hostilities*, including members of armed forces who have laid down their arms and those placed 'hors de combat' by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.[15]

This concept is found again in Article 51(3) of Additional Protocol I, signed in 1977. It states that civilians shall not be the object of attack

---

[14] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

[15] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 3, Aug. 12, 1949, 6 U.S.T. 3314, 75 U.N.T.S. 31 [hereinafter GC I]; Convention on the Wounded, Sick and Shipwrecked of Armed Forces at Sea art. 3, 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 art. 3, 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 art. 3, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV] (emphasis added); *see also* INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 1013 (Nils Melzer ed., 2009) [hereinafter ICRC INTERPRETIVE GUIDANCE], *available at* http://www.icrc.org/eng/assets/files/other/irrc-872-reports-documents.pdf.

"unless and for such time as they take a direct part in hostilities."[16] Whereas Common Article 3 applies to non-international armed conflicts, Article 51(3) of Additional Protocol I is applicable to international armed conflicts; both are considered customary international law.[17]

A definition of what specifically constitutes direct participation in hostilities, however, is not provided in either the Geneva Conventions or Additional Protocols. The International Committee of the Red Cross (ICRC) Commentary on Additional Protocol I suggests a definition, stating that "[d]irect participation means acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces."[18] This strict—and controversial—interpretation is not found in any treaty, however, and is not customary international law.[19]

The lack of clear guidance regarding what acts comprise direct participation in hostilities becomes increasingly troublesome in modern conflicts. Developments in weapons technology and the asymmetric nature of many armed conflicts have resulted in a growing number of civilians directly participating in hostilities; for example the farmer-by-day-but-fighter-by-night civilian technical specialists who is effectively intermingled with armed forces, as well as the contractors who are the beneficiaries of the outsourcing of military functions.[20] This has led to uncertainty as to how to distinguish between legitimate military targets and persons protected from direct attack. For this reason, the ICRC held

---

[16] AP I, *supra* note 14, art. 51.3.

[17] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 1013–14; *see also* U.S. DEP'T OF THE NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS sec. 8-2 (2007) [hereinafter NWP 1-14M]. *But see* PRESIDENT RONALD REAGAN, MESSAGE FROM THE PRESIDENT OF THE UNITED STATES TRANSMITTING THE PROTOCOL II ADDITIONAL TO THE GENEVA CONVENTIONS OF AUGUST 12, 1949, S. TREATY DOC NO. 100-2, at III-IV (Jan. 29, 1987) (noting that the United states "cannot ratify . . . Protocol I," which "is fundamentally and irreconcilably flawed," because, in part, it "would grant combatant status to irregular forces even if they do not satisfy the traditional requirements" of the law of armed conflict).

[18] INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (1987) [hereinafter ICRC COMMENTARY].

[19] Ian Henderson, Letter to the Editor: Status of the ICRC Commentaries, JUST SEC., Nov. 20, 2013, *available at* http://justsecurity.org/2013/11/20/letter-editor-status-icrc-commentaries/.

[20] *See* Michael N. Schmitt, *War, Technology, and International Humanitarian Law*, PROGRAM ON HUMANITARIAN POL. AND CONFLICT RESEARCH AT HARV. UNIV. 2005, at 5 (Occasional Paper Series, Ser. No. 4, 2005).

five meetings between 2003 and 2008 at The Hague and in Geneva in order to come to a consensus on how to define direct participation in hostilities.[21]

1. ICRC Interpretive Guidance

In order to achieve an international consensus on a definition of direct participation in hostilities, the ICRC brought together fifty experts in IHL from international organizations and military, governmental, and academic circles.[22] They were asked to address the following three questions: "(1) Who is considered a civilian for the purposes of conducting hostilities?; (2) What conduct amounts to direct participation in hostilities?; and (3) What are the precise modalities according to which civilians directly participating in hostilities lose their protection against direct attack?"[23]

The product of these discussions was the *ICRC Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (*ICRC Interpretive Guidance*), published in 2009. This guidance proposes a far more expansive definition of direct participation in hostilities than that proffered in the 1987 ICRC Commentary on Additional Protocol I. Instead of limiting direct participation to acts that are likely to cause actual harm, the ICRC Interpretive Guidance states: "In order to qualify as direct participation in hostilities, a specific act must . . . be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack."[24] Once this threshold of harm is reached, the *ICRC Interpretative Guidance* argues that those individuals lose their protected status as civilians and are no longer entitled to protection against direct attack for the duration of the hostile act.[25]

In addition to the threshold of harm, the *ICRC Interpretative Guidance* suggests that there are two additional cumulative criteria that

---

[21] *Civilian "Direct Participation in Hostilities": Overview*, INT'L COMM. OF THE RED CROSS (Oct. 29, 2010), http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/participation-hostilities/overview-direct-participation.htm.
[22] *Id.*
[23] *Id.*, *see also* ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 991–92.
[24] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 995.
[25] *Id.* at 996.

must be met to qualify as direct participation in hostilities: direct causation and belligerent nexus. Direct causation refers to the causal link between the act and the harm likely to result from that act. Belligerent nexus refers to the concept that the act must be specifically intended to directly cause the required threshold of harm to the detriment of a party to the conflict. Also of note is that the *ICRC Interpretative Guidance* states that the commission of an act of direct participation in hostilities includes the time for preparatory measures, as well as the time necessary to return from the location of its execution. However, once the act is complete, the *ICRC Interpretative Guidance* argues, that individual regains his or her protected status as a civilian and can no longer be targeted.[26]

2. Criticism of ICRC Interpretive Guidance

Following the publication of the *ICRC Interpretive Guidance*, several of the experts who participated in the meetings that led to its publication publically criticized the final product. The majority of the criticism was directed at two topics that are not addressed in this article: the guidance's discussions of status-based identification and restraints on the use of force.[27] But there are two relevant criticisms of the criteria.

With regards to the first criterion—threshold of harm—one valid criticism is that the requirement that the act must be likely to "adversely affect" military capacity illogically excludes certain civilian actions.[28] Specifically, the language excludes inverse scenarios—specific acts likely to favorably affect military capacity. Dr. Michael Schmitt, who

---

[26] *Id.*

[27] *See, e.g.*, Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT'L SEC'Y J. 5, 8 (2010) *available at* http://harvardnsj.org/2010/05/the-interpretive-guidance-on-the-notion-of-direct-participation-in-hostilities-a-critical-analysis/ (stating that discussions during the formation of the guidance regarding the status-based distinction of civilians participating in organized armed groups was "the greatest source of controversy" and that restraints on the use of force "attracted the greatest criticism"); W. Hays Parks, *Part IX of the ICRC 'Direct Participation in Hostilities' Study: No Mandate, No Expertise, and Legally Incorrect*, 42 INT'L L. & POL. 769 (2010) (referring to the section in the ICRC Interpretive Guidance that addresses restraints on force); Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641 (2010) (criticizing the ICRC Interpretive Guidance treatment of membership in organized groups).

[28] Schmitt, *supra* note 27, at 9; ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 1016.

was a member-turned-critic of the process of creating the *ICRC Interpretive Guidance*, highlights this distinction with the example of IEDs. The current threshold of harm would include burying an IED on a road used by opposing forces because the act would adversely affect opposition military capacity. However, the threshold would not include providing training to friendly forces on how to assemble and use Improvised Explosive Devices (IEDs).[29]

A closely-aligned criticism can be made against the belligerent nexus criterion. The *ICRC Interpretive Guidance* defines the nexus as an act "in support of a party to the conflict and to the detriment of another," but Dr. Schmitt proposes that the language "be framed in the alternative: an act in support or to the detriment of a party"; this would, he argues, include specific acts designed to adversely affect one party to the conflict without intending "to assist its opponent."[30] Arguably, assisting one party would almost always be a detriment the other; therefore, this criticism is relatively benign.

Although major criticism of some aspects of the *ICRC Interpretive Guidance* exists, the absence of major criticism of the three criteria proposed by the guidance to determine direct participation in hostilities is a testament to their usefulness. The three criteria are an effective tool for identifying civilians who are directly participating in hostilities under the LOAC. The criteria establish a workable baseline for accepted norms of state behavior, even though those criteria have not been accepted by any state, to include the United States.[31]

3. The United States' Position on Direct Participation in Hostilities

The United States' position on what specific acts constitute direct participation in hostilities must be gleaned from several sources. Each branch of the armed services has definitions that differ slightly from each other in this area. The Standing Rules of Engagement (SROE) that apply to all services provide an analysis based on hostile act and hostile

---

[29] Schmitt, *supra* note 27, at 10.
[30] *Id.* at 34.
[31] INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, THE LAW OF ARMED CONFLICT DESKBOOK 145 (2013).

intent.[32] Read holistically, the U.S. position on direct participation in hostilities sets a higher threshold than the criteria proposed by the *ICRC Interpretive Guidance* and lacks the functional clarity of the three criteria test.

a. Service Doctrine

With regards to the concept of direct participation in hostilities, the Army Field Manual on the *Law of Land Warfare* contains language similar to that addressed in the *ICRC Interpretive Guidance*. However, the Army Field Manual uses broad language without further explanatory guidance. Specifically, the manual states that if "an individual protected person is definitely suspected of or engaged in activities hostile to the security of the State, such individual person shall not be entitled to claim such rights and privileges under the present Convention as would, if exercised in the favour [*sic*] of such individual person, be prejudicial to the security of such State."[33] Additionally, the manual states that:

> Persons who, without having complied with the conditions prescribed by the laws of war for recognition as belligerents . . . commit hostile acts about or behind the lines of the enemy are not to be treated as prisoners of war and may be tried and sentenced to execution or imprisonment. Such acts include, but are not limited to, sabotage, destruction of communications facilities,

---

[32] CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT (SROE)/STANDING RULES FOR THE USE OF FORCE (SRUF) FOR U.S. FORCES (13 June 2005) [hereinafter SROE].

[33] U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE para. 550 (18 July 1956) [hereinafter FM 27-10], *available at* http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm27_10.pdf. The full text reads:

> A neutral cannot avail himself of his neutrality:
>
> a. If he commits hostile acts against a belligerent.
>
> b. If he commits acts in favour of a belligerent, particularly if he voluntarily enlists in the ranks of the armed force of one of the parties. In such a case, the neutral shall not be more severely treated by the belligerent as against whom he has abandoned his neutrality than a national of the other belligerent State could be for the same act.

Id.

> intentional misleading of troops by guides, liberation of prisoners of war, and other acts not falling within Articles 104 and 106 of the Uniform Code of Military Justice and Article 29 of the Hague Regulations.[34]

The threshold of harm established by the Army Field Manual is therefore the commission of either a hostile act or of activities hostile to the security of the State—language that is more vague, as well as more restrictive, than the definition proposed in the *ICRC Interpretive Guidance*.

The U.S. Air Force does not directly address the treatment of civilians who participate in hostilities. The Air Force operations doctrine briefly discusses the principles of LOAC in its annex pertaining to targeting. The discussion, however, mainly states that targeting civilians is prohibited without delving into the nuances of direct participation.[35]

The U.S. Navy doctrine pertaining to civilian combatants, contained in the *Commander's Handbook on the Law of Naval Operations*, offers the most thorough discussion of civilian participation in armed conflict. This doctrine is also applicable to the U.S. Marine Corps and U.S. Coast Guard.[36] Specifically, the publication states: "[u]nlawful combatants who are not members of forces or parties declared hostile but who are taking a direct part in hostilities may be attacked while they are taking a direct part in hostilities, unless they are *hors de combat*."[37] Although the publication does not directly define 'a direct part in hostilities,' it does provide examples of qualifying actions. The examples are: "taking up arms"; attempting to "kill, injure, or capture enemy personnel"; destroying property; "serving as lookouts or guards"; and serving as "intelligence agents."[38] It further states that the determination should be made on a "case-by-case basis" based on "the person's behavior, location and attire, and other information available at the time."[39] This definition

---

[34] *Id.* para. 81.
[35] U.S. DEP'T OF AIR FORCE, DOCTRINE DOC. 3-60, TARGETING para. 33 (8 June 2006) [hereinafter AFDD 3-60]. *But see* GEORGE N. WALNE, INTERNATIONAL LAW-THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, *in* U.S. DEP'T OF AIR FORCE, PAM 110-31, Professional Paper 457, November 1987, *available at* http://www.cna.org/sites/default/files/research/5500045700.pdf (stating that civilians enjoy protection of the law until "such time as they take a direct part in hostilities").
[36] NWP 1-14M, *supra* note 17.
[37] *Id.* para. 8.2.
[38] *Id.*
[39] *Id.*

provides more clarity than what is found in Army and Air Force doctrine. It is nonetheless more restrictive than the ICRC position. By using the term "enemy personnel," the Navy definition does not include acts of harm against other civilians. Nor does the definition include other acts likely to adversely affect military operations or military capacity.[40]

The differences in each Armed Service's treatment of direct participation in hostilities, as well as their shared failure to adequately define what acts would constitute direct participation in hostilities, beyond several non-inclusive examples, creates a persuasive argument in favor of using the definition contained in the *ICRC Interpretive Guidance*. However, the SROE, promulgated by the Chairman of the Joint Chiefs of Staff and applicable to all Armed Services, avoids the slippery definition of "direct participation" by ignoring it all together.[41]

b. Standing Rules of Engagement

The SROE applies to all U.S. forces engaged in military operations outside of the United States and within the United States in the case of homeland-defense missions.[42] The SROE was designed to be consistent with LOAC; however, because the rules also reflect national policy, "they often restrict combat operations far more than do the requirements of international law."[43] The rules of engagement pertaining to conduct-based targets illustrate this restriction.

The rules allow for conduct-based engagement of individuals who commit a hostile act or demonstrate a hostile intent against U.S. forces. A hostile act is defined as: "an attack or other use of force against the United States, U.S. forces or other designated persons or property [and] force used directly to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital [United States Government] property."[44] This definition is similar to the definition proposed by the *ICRC Interpretive Guidance*, specifically as it pertains to actions that directly affect military operations. However, the

---

[40] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 996.
[41] SROE, *supra* note 32.
[42] *Id.* at 1.
[43] NWP 1-14M, *supra* note 17, para. 4.4.
[44] SROE, *supra* note 32, encl. A. Although many portions of the SROE are classified, Enclosure A, which contains the specific rules of engagement, is unclassified.

ICRC Interpretive Guidance interprets LOAC to also permit any actions likely to adversely affect military operations, which is broader in scope than the SROE definitions of hostile act or hostile intent.

The SROE defines hostile intent as: "the threat of imminent use of force against the United States, U.S. forces or other designated persons or property [and] the threat of force to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital USG property."[45] Although this definition addresses individual conduct that has the intended effect of impeding military operations, it is nonetheless more restrictive than the "likely to" standard found in the *ICRC Interpretive Guidance*. The notable restriction in this definition is that an individual who intends his or her actions to impede a military mission cannot be engaged unless his or her actions pose an "imminent" threat. The definition of what constitutes an imminent threat, however, is unclear. The SROE defines imminent use of force as "not necessarily . . . immediate or instantaneous."[46] This implies that the threatened use of force could be less than immediate; however, the SROE contains no further clarification other than stating that the determination of whether a threat is imminent should be "based on an assessment of all facts and circumstances known to U.S. forces at the time."[47]

By qualifying hostile intent with imminent threat, the SROE places more restrictions on military personnel than the LOAC. Although the phrase "direct participation in hostilities" does not appear in the SROE, the definitions of hostile act and hostile intent are similar to the definitions proposed by the *ICRC Interpretive Guidance* and are, therefore, well within the boundaries of the law of armed conflict.

B. The Applicability of Direct Participation in Hostilities Analysis to Cyber Acts

1. U.S. Policy

The U.S. position on the application of LOAC to cyberspace was first articulated in the 2011 White House International Strategy for Cyberspace, which stated that, "[T]he development of norms for state

---

[45] *Id.*
[46] *Id.*
[47] *Id.*

conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[48]

This position was further affirmed during an address by State Department Legal Adviser Harold Koh at the 2012 Cyber Command Legal Conference. He stated that the U.S. government's position is that existing international laws of armed conflict apply to cyberspace and that this should be the starting place for any further analysis on how those laws will practically apply to cyberspace.[49]

A glimpse into how the government views the applicability of LOAC to cyber hostilities that are committed by non-state actors is contained in a memorandum from the Vice Chairman of the Joint Chiefs of Staff containing a list of cyberspace terminology.[50] Included in the list are definitions of hostile act and hostile intent that have been tailored to cyber operations.

In that memorandum, hostile act is defined as:

> Force or other means used directly to attack the U.S., U.S. forces, or other designated persons or property, to include critical cyber assets, systems or functions. It also includes force or other means to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital U.S. Government property.[51]

The definition is essentially a duplicate of the definition of hostile act located in the SROE, except that it adds "cyber assets, systems or

---

[48] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 7, at 9.

[49] Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm; *see also* U.S. DEP'T OF AIR FORCE, DOCTRINE DOC. 3-12, CYBERSPACE OPERATIONS (30 Nov. 2011) (stating that the law of armed conflict applies to the "employment of cyberspace capabilities").

[50] Memorandum from Vice Chairman of the Joint Chiefs of Staff to Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates, subject: Joint Terminology for Cyberspace Operations (Nov. 28, 2010) [hereinafter Joint Terminology for Cyberspace Memo].

[51] *Id.* at 9.

functions." Thus, if a non-state actor were to attack a cyber asset, system, or function, such as a shipboard navigation system, that would be considered a hostile act to the same extent as an attack on the ship itself.

Hostile intent is defined as:

> The threat of an imminent hostile act. Determination of hostile intent in cyberspace can also be based on the technical attributes of an activity which does not meet the hostile act threshold but has the capability, identified though defensive countercyber or forensic operations, to disrupt, deny, degrade, manipulate, and/or destroy critical cyber assets at the will of an adversary (such as a logic bomb or 'sleeper' malware). Because an individual's systems may be used to commit a hostile act in cyberspace without their witting participation, the standard for attribution of hostile act/intent for defensive counter-cyber purposes is "known system involvement," and is not witting actor or geography-dependent.[52]

Only the first sentence of this definition reflects the SROE; what follows is additional language apparently tailored to meet the challenges of stopping attacks before they occur in an environment where an attack can be launched and executed in nanoseconds. An arguable example would be if a counter-cyber operation identifies that a known hacker named Q-T has developed the capability to create a worm that can disable the navigation systems of U.S. naval vessels—prior to him actually completing the worm or loading it onto a USB flash drive—Q-T would be demonstrating hostile intent. The language in the definition suggests that when determining hostile intent in cyberspace, the mere possession of the capability to adversely affect critical cyber assets will satisfy the imminence requirement.

The policy remarks and cyber terminology provide a starting point for applying a direct-participation-in-hostilities analysis to cyber hostilities committed by civilians. More is needed, however, in order to identify these individuals with any degree of certainty within a LOAC construct. The *Tallinn Manual* is helpful in developing a baseline for a LOAC construct as it pertains to cyber warfare.

---

[52] *Id.* at 10.

2. Tallinn Manual

As discussed briefly in the introduction, the previously unexplored world of cyber law as applied to LOAC has recently been examined in detail by a group of international experts, who subsequently published the *Tallinn Manual*. Published in 2013, the *Tallinn Manual* takes, *inter alia*, the concepts of distinction and direct participation in hostilities and applies them to cyber scenarios.[53] The international group of experts who prepared the *Tallinn Manual* took a position in line with former State Department Legal Adviser Harold Koh's comments at the 2012 Cyber Command Legal Conference by fully applying the existing international legal regime to cyber warfare.[54] The manual also borrows heavily from the *ICRC Interpretive Guidance* in the area of civilian participation in hostilities.[55] It therefore bridges U.S. policy and the *ICRC Interpretive Guidance*, providing a useful tool in evaluating hostilities in cyberspace under LOAC.

Rule 34 of the *Tallinn Manual* delineates four groups of persons who may be the object of cyber attacks: (1) members of the armed forces; (2) members of organized armed groups; (3) civilians taking a direct participation in hostilities; and (4) civilians participating in a *levée en masse* in an international armed conflict.[56]

The first two classifications are status-based distinctions; the latter two are conduct-based distinctions.[57] Whereas the *ICRC Interpretive Guidance* concluded that civilians may only be targeted based on conduct, the *Tallinn Manual* offers an interesting exception concerning civilian contractors. The participants agreed that individual civilian contractors may only be targeted if they are directly participating in hostilities; however, the commentary to Rule 34 identifies a divide

---

[53] TALLINN MANUAL, *supra* note 12, at 4–6.

[54] *See* Koh, *supra* note 49; Schmitt, *supra* note 13; *see also* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13 (2012), *available at* http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

[55] TALLINN MANUAL, *supra* note 12, at 119 nn.63–65.

[56] *Id.* at 115.

[57] The International Group of Experts who prepared the *Tallinn Manual* was divided over the distinction of members of an organized armed group. Some participants argued that mere membership in an organized armed group suffices for individual members to be targeted. However, others argued, consistent with ICRC guidance, that only members who are continuously performing a combat function within those groups may be targeted. *See id*. at 116.

between the participants on the issue of whether this is also true for civilian companies that have been contracted by a party to the conflict to perform cyber attacks in support of military operations. The majority agreed that these companies would qualify as an organized armed group such that they can be targeted at any time based on their status.[58] The minority view is that a contractual relationship is an insufficient basis to classify such companies as organized armed groups. The minority view nonetheless acknowledged that individual members of such a company could be targeted if and when they became direct participants in hostilities.[59]

In defining what acts qualify as direct participation in hostilities, the participants in the *Tallinn Manual* generally agreed with the three criteria set forth in the *ICRC Interpretive Guidance*: threshold of harm, causal link, and belligerent nexus.[60]

a. Threshold of Harm

The first criterion for determining whether a civilian has directly participated in hostilities, discussed above, is the threshold for harm. The *Tallinn Manual* definition of this criterion is closely aligned with the definition proposed by the *ICRC Interpretive Guidance*: "the act (or closely related series of acts) must have the intended or actual effect of negatively affecting the adversary's military operations or capabilities, or inflicting death, physical harm, or material destruction on persons or objects protected against direct attack."[61]

The one notable difference between the *Tallinn Manual* definition and the *ICRC Interpretive Guidance* is the *Tallinn Manual*'s use of the word "intent." The *ICRC Interpretive Guidance* refers instead to actions "likely to" affect military operations.[62] By directly referring to the *ICRC Interpretive Guidance* definition, the *Tallinn Manual* appears to treat the difference in language as semantic; however, the *Tallinn Manual* is

---

[58] *Id.* at 117-18.
[59] *Id.*
[60] *Id.* at 119; *see also* ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 47, 51, 58.
[61] TALLINN MANUAL, *supra* note 12, at 102; *see also* ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 47.
[62] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 995.

broader in scope. [63] For example, a worm can be designed with the intent to disrupt military capabilities but have no likelihood of success due to a fault in its design. Under the *Tallinn Manual* definition, the intended effect would satisfy the threshold of harm. But because the worm was not likely to—or even, could not—actually affect military operations, it would not satisfy the *ICRC Interpretive Guidance* definition.

Applying this criterion to cyber activities, the *Tallinn Manual* suggests that civilians engaging in cyber operations that disrupt the enemy's command and control would be lawful targets. A less obvious minority view is that acts that enhance one's own military cyber assets would also be included because the logical result of those acts would be a weakening of the adversary's relative position.[64] Expanding on this view, one can envision a number of seemingly non-belligerent scenarios that could qualify as direct participation in hostilities. For example, a civilian information technology specialist who loads updates to a military network in order to enhance its security could theoretically be a lawful target – at least if the remaining two criteria are met.

Applying the threshold of harm to the hypothetical attack on the USS *Bonhomme Richard*, the act of using a worm to control and disrupt the ship's navigation system had the actual effect of adversely affecting both the ship's military operations and the military capability of the 31st MEU. The actions of LulzKhat would therefore satisfy the first criterion for determining direct participation in hostilities.

There are two additional hypothetical participants whose actions should be considered in this scenario: the individual who created the worm and the individual who sold the USB drive to the unsuspecting sailor. Assume for this scenario that LulzKhat is an associate of an individual who operates under the alias Q-T. Q-T designed the worm for the express purpose of infiltrating U.S. Navy navigation systems. Tony Chee operates a small shop near the Singapore port that caters to sailors and was the one who sold the infected USB drive to the sailor attached to the USS *Bonhomme Richard*. The actions of both Q-T and Tony Chee—by respectively creating the worm and selling the device that transported the worm—had the actual effect of adversely affecting the military operations and the 31st MEU. Therefore, the actions of those individuals would also meet the threshold of harm.

---

[63] TALLINN MANUAL, *supra* note 12, at 119 n.63.
[64] *Id.* at 120.

b. Causal Link

The second criterion that must be met is a causal link, meaning that there must be a causal link between the harmful act and the intended or actual results of that act. The manual offers a single broad example, a cyber operation (the act) that directly results in the disruption of an enemy's command and control network (the result). [65] Additional examples could include creating and uploading malware that directly results in the shutdown of an enemy's electric grid; gathering information on enemy operations through cyber means that directly assists one's own forces; or designing malware that identifies and exploits vulnerabilities in the enemy's computer system.

The actions of LulzKhat represent a clear causal link between act and result. The act committed by LulzKhat is his use of the worm to take control of the USS *Bonhomme Richard*'s navigation system, directly resulting in the system being rendered inoperable. Establishing a causal link between the actions of the other two hypothetical actors is not as succinct.

Consider this alternative: Q-T created the worm days before the attack, however, he did so knowing only that it was going to be used for an attack generally, and had no knowledge of the specifics of the attack. The *Tallinn Manual* addresses a similar scenario and acknowledges that no clear consensus was reached amongst the participants as to whether a causal link could sufficiently be established under these circumstances. The direct participation in hostilities analysis provided by the U.S. Navy *Commander's Handbook on the Law of Naval Operations* is more useful in this context. The handbook states that "an honest determination" should be made based on information available at the time to determine whether a person is directly participating in hostilities. [66] An honest determination can be made that there is a causal link between Q-T's actions and the resulting harm based on temporal proximity, the tailored construction of the worm, and the relationship between Q-T and LulzKhat.

The third hypothetical actor, Tony Chee, acted by selling the infected USB drive to the U.S. sailor. The infiltration of the ship's computer systems was directly caused by the sale of the USB drive to a sailor

---

[65] *Id.* at 119–20.
[66] NWP 1-14M, *supra* note 17.

belonging to that ship. Thus there is a casual link. Despite that link, though, Tony Chee's knowledge—or lack thereof—of the presence of a worm on the drive or its purpose is relevant to the final criterion.

c. Belligerent Nexus

The third criterion is a belligerent nexus—that the acts are directly related to hostilities in situations of international or non-international armed conflict. As noted in the *ICRC Interpretive Guidance*, the concept of direct participation in hostilities cannot refer to conduct occurring outside of either an international or non-international armed conflict.[67] For example, if a civilian uses cyber assets to siphon a large amount of funds from a party to a conflict for personal gain, that act does not meet the belligerent-nexus criterion. This remains true even if the theft causes a direct adverse affect to the victim's military capability because the purpose of the act was not to support one party to the conflict by harming another. However, if the purpose of the theft was to benefit a belligerent party to the conflict (e.g., to buy weapons for ISIL or purchase IED-making equipment for an insurgent group), the civilian committing the theft would be directly participating in hostilities and would lose his protected civilian status.[68]

Why does this distinction matter? In the first scenario, the thief would be classified as a criminal and would, therefore, be subject to the pertinent criminal-justice system. In the second scenario, the thief would be a direct participant in an armed conflict and would therefore be a lawful target.

Objectively, the actions of the pseudonymous LulzKhat directly disrupted the capability of the 31st MEU to conduct their mission. Whether a belligerent nexus exists between his actions and the resulting disruption depends upon LulzKhat's subjective intent. If, for example, LulzKhat's intent was to simply demonstrate his ability to subvert a military network for the purpose of gaining credibility amongst his peers, he would not be a direct participant in hostilities. Getting into the mind of an individual—especially an individual sequestered behind a computer terminal in an unknown location—is not a straightforward task. Again, the U.S. Navy's "honest determination" standard is most helpful in these

---

[67] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 1012.
[68] *See* TALLINN MANUAL, *supra* note 12, at 120.

or similar scenarios.[69] An examination of the information available to U.S. forces following the attack about LulzKhat's associates, communications, and previous activities, for example, could result in an honest determination that he disabled the navigation systems to aid the terrorist organization that committed the attack on Subic Bay.

A similar analysis could be made to determine the subjective motives of the worm designer, Q-T, and the shop vendor, Tommy Chee. It is possible to conclude that even if Tommy Chee was aware that the items he sold contained malware, if his main motivation for selling those items was to make a personal profit, he may not be considered a direct participant in hostilities.

Neither the *Tallinn Manual* nor the *ICRC Interpretive Guidance* provides specific tools for determining a civilian participant's subject intent. Commanders and other lawful combatants engaged in hostilities must rely on honest judgment and make decisions based on available information. However, decisions in cyberspace must be made swifter than those on a conventional battlefield. Because of the speed at which a hostile act can occur via cyber assets, determining the duration of a civilian's participation in cyber hostilities can be complex.

d. Duration of Participation

The *Tallinn Manual*, adopting the language of the *ICRC Interpretive Guidance*, proposes that a civilian is "targetable for such time as he or she is engaged in the qualifying act of direct participation."[70] The *ICRC Interpretive Guidance* concluded that the targeting window encompasses the act, the preparatory time to commit the act, and the travel to and from the place where the act was committed.[71] For example, a civilian who leaves his shop and picks up his rifle at sunset, walks several miles to an enemy road block and fires upon it, walks home, and then puts his rifle away at sunrise is a lawful target from sunset to sunrise. Applying that guidance to cyber hostilities is more complex.

If, in the above scenario, you exchange 'rifle' for 'thumb drive containing malware' and 'enemy road block' for 'computer with access

---

[69] NWP 1-14M, *supra* note 17.
[70] TALLINN MANUAL, *supra* note 12, at 120–21.
[71] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 996.

to enemy systems,' the sunset to sunrise targeting window would remain unchanged. However, does preparatory time include the time it took to create the malware or the time it took to probe the enemy's systems for vulnerabilities susceptible to malware? The answer is unclear. Equally as vague is the "travelling from" time. As noted in the *Tallinn Manual*, a hallmark of cyber hostilities is their delayed effects.[72] An example provided in the manual is the emplacement of a logic bomb designed to activate at some future point.[73]

There was a split in opinion among the contributors to the *Tallinn Manual* on how to address these targeting-window issues. The majority took the position that direct participation in cyber hostilities begins with mission planning (e.g., probing the enemy's systems) and ends "when the individual terminates *an active role* in the operation."[74] An individual's active role is complete once, for example, the malware is uploaded or logic bomb is emplaced even though the actual damage to the enemy's systems may not occur until a later point in time. The distinction between the majority and minority views is whether direct participation continues after emplacement in cases in which activation is remote. The majority view is, yes; the active role of the participant is not completed until he or she activates the logic bomb.[75] The minority view, however, is that the act of emplacement and the subsequent act of activation are separate acts of direct participation.[76]

Applying this analysis to the introductory scenario, a factor necessary to determine the duration of worm developer Q-T's participation is when he began designing the worm. If he created the worm and delivered it to LulzKhat six months before its use and played no further active role in the operation, Q-T's participation ended once he delivered the malware. If Q-T continued to take an active part in the operation—for example, by monitoring updates to cyber-security systems to update his worm if needed—those actions would lengthen the duration of his participation.

---

[72] TALLINN MANUAL, *supra* note 12, at 121.
[73] *Id.*
[74] *Id.* (emphasis added).
[75] However, this is to be distinguished from a logic bomb or other malware that activates automatically based on a predetermined length of time or upon the performance of a particular action by the target system. *See id.*
[76] *Id.*

Despite the existence of opposing majority and minority views within the *Tallinn Manual*, it provides a workable framework for identifying civilian (or non-state actor) participation in cyber hostilities. Whereas the current U.S. policy—that LOAC applies to cyber war—provides a baseline for analysis, the *Tallinn Manual* offers practical interpretations of LOAC applicability based on accepted norms of international law.

C. Once We Have Identified Them, What Should We Call Them?

A civilian who directly participates in hostilities though the use of cyber assets to support terrorism deserves a name less cumbersome than a legal description. This article proposes: cyberterrorist. The use of the term cyberterrorist is often used to describe individuals who should be more accurately termed cybercriminals.[77] In the context of LOAC, a clear distinction must be made between cybercriminals and cyberterrorists because that distinction determines whether an individual can be lawfully targeted under international law—vice arrested and prosecuted pursuant to domestic law. The direct-participation-in-hostilities analyses proposed by the ICRC and the *Tallinn Manual* provide a concise method of distinguishing the two categories of actors.

1. Cybercriminals

The *Webster's New World Hacker Dictionary* defines "cybercriminal" as an individual who commits "crimes completed either on or with a computer."[78] This definition is straightforward but

---

[77] *See, e.g.*, Sarah Gordon, *Cyberterrorism*, SYMANTIC SECURITY RESPONSE (2003), *available at* https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (discussing the varying usages and definitions of 'cyberterrorism' found in policy and media).

[78] WEBSTER'S NEW WORLD HACKER DICTIONARY 80 (Bernadette Schell & Clemens Martin eds., 2006) [hereinafter HACKER DICTIONARY]. (The definition provides the following examples: "Cybercrime involves such activities as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing, and trademark protection; overriding encryption to make illegal copies; software piracy; and stealing another's identity to perform criminal acts."); *see also* Zeviar-Geese, G., *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet* (2004), *available at* http://law.gongzaga.edu/borders/documents/cyberlaw.htm.

nonetheless too broad to be useful in the context of international armed conflict.

A more useful definition in an international-law context can be determined by applying the *ICRC Interpretive Guidance* to cyber scenarios. Using the *ICRC Interpretive Guidance*, a cybercriminal would be any individual who commits an illegal act that fails one of the three criteria of the ICRC direct-participation-in-hostilities analysis. [79]

If, for example, a cyber actor attacks a civilian computer network that shuts down Amazon.com for a day, causing widespread civilian nuisance and a large profit loss to the American-based company, the actor would be considered a cybercriminal because the act would fail to meet the threshold of harm required to constitute an attack.

If the cyber actor in the above scenario creates a virus intended to disrupt Amazon.com but causes a cascade of events that eventually results in a disruption to a military network, the actor would still be considered a cybercriminal because the direct causation prong would not be met.

Finally if a cyber actor commits an act that meets the previous two prongs (i.e. adversely affects military operations via direct causation) but the intent of the act is for material gain, such as the theft scenario discussed *supra*, the individual remains a cybercriminal.

2. Cyberterrorists

The National Infrastructure Protection Center (NIPC), which is part of the Department of Homeland Security, defines cyberterrorism as "a criminal act conducted with computers and resulting in violence, destruction, or death of targets in an effort to produce terror with the purpose of coercing a government to alter its policies."[80] This definition is inadequate when applied to the realm of international armed conflict because it is based on criminal acts. This article submits that a more applicable definition of a cyberterrorist is a non-state actor who uses

[79] ICRC INTERPRETIVE GUIDANCE, *supra* note 15.
[80] HACKER DICTIONARY, *supra* note 78, at 87.

cyber assets to directly participate in hostilities in support of al-Qaeda, the Taliban, and associated forces, to include ISIL.[81]

The proposed definition is at odds with how the *Tallinn Manual* addresses cyber acts of terror. The *Tallin Manual* addresses "terror attacks" in Rule 36 but only in the context of the principle of distinction as applied to a party to a conflict.[82] Specifically, the *Tallin Manual* defines "terror attacks" as "cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population."[83] The commentary to this rule states that it is based on both Article 51(2) of Additional Protocol I and Article 13(2) of Additional Protocol II.[84] As submitted in the *ICRC Commentary to the Additional Protocols*, the purpose of Article 51(2) is "to prohibit acts of violence, the primary purpose of which is to spread terror, *without offering substantial military advantage*."[85] Notably, neither the plain language of Article 51(2) nor the commentary contemplates the actions of a civilian spreading terror among a civilian population during an armed conflict. Both make an assumption that the civilian population need only be protected from armed forces. This assumption does not accord with contemporary reality, wherein non-state actors use suicide vests in markets or threaten the use of bombs on planes for the purpose of spreading terror amongst a civilian population in support of one party to the conflict and to the detriment of the other. Although an attack against civilians for the purpose of spreading terror would constitute direct

---

[81] *See, e.g.*, 2010 NATIONAL STRATEGIC STRATEGY, *supra* note 1 (The United States is still in an international armed conflict with the Taliban, al-Qaeda, and associated forces.); Press Release, The White House, Office of the Press Secretary, Fact Sheet: The President's May 23 Speech on Counterterrorism (May 23, 2013) [hereinafter May 23 Speech on Counterterrorism], *available at* http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-president-s-may-23-speech-counterterrorism.

[82] TALLINN MANUAL, *supra* note 12, at 122–24; *see also* AP I, *supra* note 14, art. 51(2).

[83] TALLINN MANUAL, *supra* note 12, at 122–24.

[84] *Id.*; *see also* AP I, *supra* note 14, art. 51(2). The full text of Article 51(2) is, "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited." *See also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13(2), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. The full text of Article 13(2) is, "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited." *Id.*

[85] TALLINN MANUAL, *supra* note 12, at 122–124 (emphasis added); *see also* ICRC COMMENTARY, *supra* note 18, para. 1940.

participation in hostilities under the *ICRC Interpretive Guidance*, a threat of such an attack would not.[86] The result is a gap in the protection for civilians against terror threats.

This gap also appears when juxtaposing the *Tallinn Manual* definition of cyberterror attacks with its definition of a cyber attack that constitutes direct participation in hostilities. For example, a cyber attack committed by a non-state actor can be considered direct participation in hostilities without affecting a military objective if it results in death, injury, or destruction to protected persons or objects.[87] However, an act of cyber terror committed by a party to the conflict, per the *Tallinn Manual* definition, need not actually result in harm—the mere threat of harm made with the purpose of spreading terror among a civilian population is sufficient. The example provided in the commentary to Rule 36 of the *Tallinn Manual* is a threat to use a cyber attack to disable a city's water distribution system.[88] The *Tallinn Manual* places the focus of determining whether the act is a terror attack on the purpose of the attack—to cause fear—not the resulting harm.

The problem with the *Tallinn Manual*'s definition of cyberterror attacks is that it creates two unequal categories of cyber actors: (1) members of an armed force that is a party to the conflict who would be in violation of international law for spreading terror, and (2) non-state actors who, according to the *ICRC Interpretive Guidance* and the *Tallinn Manual*, cannot be lawfully targeted for the same conduct. This is unhelpful to commanders who may encounter a non-state actor who commits an act of cyberterror that does not adversely impact military operations or capacity, or otherwise cause actual harm to civilians or civilian objects. However, because this individual falls through the gap by merely causing widespread terror via a threat of a cyber attack, vice causing actual damage or an imminent threat of damage, he must be considered a cybercriminal not subject to military targeting.

---

[86] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 995.
[87] TALLINN MANUAL, *supra* note 12, at 123.
[88] *Id.* at 123–24.

III. The Classification of Identified Hostile Cyber Actors, or Cyberterrorists, Under the Law of Armed Conflict

A. Summary of the Concept of Classification

The Third Geneva Convention establishes two legal classifications of individuals within the context of an international armed conflict—combatants and civilians.[89] Combatant privilege, namely the right to directly participate in hostilities with immunity from domestic prosecution for lawful acts of war, is afforded only to members of the armed forces of parties to an international armed conflict (except medical and religious personnel), as well as to participants in a *levée en masse*.[90]

Although all privileged combatants have a right to directly participate in hostilities, they do not necessarily have a function requiring them to do so (e.g., admin personnel). However, individuals who assume continuous combat functions outside the privileged categories of persons, as well as in a non-international armed conflict, are not entitled to combatant privilege under the law of armed conflict.[91] This gap in protected groups creates a third classification—unlawful combatants. Although this category of persons is not recognized in the Geneva Conventions or its Protocols, it is recognized under U.S. domestic law.[92]

1. Who is Entitled to Combatant Privilege?

In order to qualify as a lawful combatant, the combatant must fall under one of the categories of lawful combatants listed in Article 4 of the Third Geneva Convention. These categories include members of the armed forces of a party to the conflict, members of militias and organized resistance movements, members of regular armed forces of a government not recognized by the detaining power, persons who accompany the armed forces, and inhabitants of a non-occupied territory who spontaneously take up arms against an invading force.[93]

---

[89] GC III, *supra* note 15, art. 4.
[90] *Id.*; AP I, *supra* note 14, art. 43(1).
[91] ICRC INTERPRETIVE GUIDANCE, *supra* note 15, at 1007.
[92] *Ex parte* Quirin, 317 U.S. 1 (1942); Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2601.
[93] GC III, *supra* note 15, art. 4. Additionally, in order to qualify as a lawful combatant members of militias or other organized resistance groups must wear a "fixed distinctive

2. Lawful Combatant Privileges

The benefit of being classified as a lawful combatant is the privileges that classification bestows upon an individual who is captured during an armed conflict. Upon capture, lawful combatants obtain prisoner of war (POW) status. Some of the many rights afforded POWs under the Third Geneva Convention include the right to refuse to answer questions other than name, rank, serial number; the right to humane treatment; and the right to immunity from personal culpability and criminal proceedings.[94] And perhaps most importantly, POWs have the right to immediate release and repatriation upon cessation of hostilities.[95]

Having a combatant privilege that distinguishes between uniformed soldiers and civilians is a necessary foundation of the law of armed conflict. As eloquently argued by Michael Walzer in his book *Just and Unjust Wars*, distinguishing between soldiers and civilians by means of external insignia is essential in order to protect civilians from attack because "soldiers must feel safe among civilians if civilians are ever to be safe from soldiers."[96]

3. Presumption of POW Status

When there is doubt as to whether an individual captured during an international armed conflict should be classified as a POW, Article 5 of the Third Geneva Convention mandates that a tribunal be held to determine the individual's status. Until that status is determined, the captured individual must be afforded the protections and privileges of a POW.[97] Article 5 of the Third Geneva Convention therefore creates a

---

sign visible at a distance"; must "carry arms openly"; must "form a part of a 'chain of command'"; and must "themselves obey the customs and the laws of war." *Id.*

[94] *Id.*

[95] *Id.* art. 118.

[96] MICHAEL WALZER, JUST AND UNJUST WARS 182 (1977).

[97] GC III, *supra* note 15, art. 5:

> The present Convention shall apply to the persons referred to in Article 4 from the time they fall into the power of the enemy and until their final release and repatriation.

presumption of POW status for belligerents captured during an international armed conflict.[98] This presumption is reflected within U.S. military doctrine.[99] United States Army Regulation 190-8, which pertains to the detention of enemy combatants and has been adopted by all U.S. military services, states:

> In accordance with Article 5, GPW, if any doubt arises as to whether a person, having committed a belligerent act and been taken into custody by the U.S. Armed Forces, belongs to any of the categories enumerated in Article 4, GPW, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.[100]

The presumption of POW status is also found in Article 45 of Additional Protocol I, which states, in part, that individuals who take part in hostilities and are captured by an adverse party "shall be presumed to be a prisoner of war."[101]

> Should any doubt arise as to whether persons, having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.

Id.

[98] *See, e.g.*, G.I.A.D. Draper, *The Status of Combatants and the Question of Guerilla Warfare*, 1971 BRIT. Y.B. INT'L L. 198 (1971).

[99] *See, e.g.*, U.S. DEP'T OF ARMY, REG. 190-8, OPNAVINST 3461.6, AfJI 31-304, MLO 3461.1, ENEMY PRISONERS OF WAR, RETAINED PERSONNEL, CIVILIAN INTERNEES AND OTHER DETAINEES (Oct. 1, 1997) [hereinafter AR 190-8], *available at* www.au.af/mil/au/awc/awcgate/law/ar190-8.pdf.

[100] *Id.* at 1-6. It further states that

> A competent tribunal shall determine the status of any person not appearing to be entitled to prisoner of war status who has committed a belligerent act or has engaged in hostile activities in aid of enemy armed forces, and who asserts that he or she is entitled to treatment as a prisoner of war, or concerning whom any doubt of a like nature exists.

Id.

[101] AP I, *supra* note 14, art. 45. The full pertinent text reads as follows:

> A person who takes part in hostilities and falls into the power of an adverse Party shall be presumed to be a prisoner of war, and therefore shall be protected by the Third Convention, if he claims the status of prisoner of war, or if he appears to be entitled to such status, or if the Party on which he depends claims such status on his behalf by

However, Article 45 of Additional Protocol I recognizes a third category of belligerent who is not addressed in the Third and Fourth Geneva Conventions, specifically "any person who has taken part in hostilities, who is not entitled to prisoner-of-war status and who does not benefit from more favorable treatment in accordance with the Fourth Convention"—namely, the unlawful combatant.[102]

B. Unlawful Combatants

What are the rights of combatants who do not qualify as privileged combatants and do not qualify as civilians? To answer this question, a definition of the term "civilian" must first be determined. The term "civilian" had no definition under LOAC until the adoption of Additional Protocol I in 1977.[103] Article 50 of Additional Protocol I defines "civilian" as:

> [A]ny person who does not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3), and (6) of the Third Geneva Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.[104]

The ICRC espouses the view that the definition of civilian found in this article is established customary international law in both

---

> notification to the detaining Power or to the Protecting Power. Should any doubt arise as to whether any such person is entitled to the status of prisoner of war, he shall continue to have such status and, therefore, to be protected by the Third Convention and this Protocol until such time as his status has been determined by a competent tribunal.

Id.

[102] *See id*. art. 45(3).

[103] *See id*. art. 50.

[104] *Id.* The articles referred to in Article 50 of AP I refers to members of the armed forces, militias and organized resistance movements belonging to a party to the conflict, GC III, *supra* note 15, art. 4(A)(1-2); members of the armed forces of a government not recognized by the Detaining Power, GC III, *supra* note 15, art. 4(A)(3); inhabitants of a non-occupied territory who spontaneously take up arms to resist invading forces, GC III, *supra* note 15, art. 4(A)(6); and all organized armed forces, groups and units under a command responsible to a party to the conflict. AP I, *supra* note 14, art. 43.

international and non-international armed conflicts.[105] But this exclusionary definition appears to run counter to the ICRC position on civilians who directly participate in hostilities. The ICRC database on International Human Rights Law addresses this dissonance by asserting that a civilian who participates directly in hostilities loses protection against attack but does not lose civilian protections upon capture.[106] Under the ICRC view, a civilian who directly participates in hostilities and is captured would not be entitled to prisoner-of-war status and instead must be tried under national law subject to fair trial guarantees.[107] Under the ICRC view, therefore, a civilian who directly participates in hostilities may, during the course of that participation, be lawfully targeted and killed without due process. However, if the adverse party decides to not avail themselves of the option of killing the civilian who is directly participating in hostilities but instead captures and detains that civilian, the civilian should be afforded all of the rights contained in the Fourth Geneva Convention pertaining to the treatment of civilians. One such right would be the right to a trial and prosecution under domestic law. This view paradoxically provides armed forces engaged in international armed conflict an incentive to choose the option to kill civilians directly participating in hostilities instead of taking the lesser means of capture and detention.

This interpretation of international law—that there is no intermediate status—has additional support. First, the Commentary to the Fourth Geneva Convention states that:

> Every person in enemy hands must have some status under international law: he is either a prisoner of war

---

[105] *Customary IHL—Rule 5. Definition of Civilians*, INT'L COMM. OF THE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule5 (last visited Jan. 4, 2014). Specifically Rule 5 states, "Civilians are persons who are not members of the armed forces. The civilian population comprises all persons who are civilians." *Id.*

[106] *Id.*

[107] *Id.* Interestingly, the ICRC definition of civilians does not include a discussion of Article 45 of AP I, *supra* note 14, which specifically states that there can be belligerents who are not entitled to either POW status or GC IV protections. Article 45 further refers to Article 75 of AP I, which lists fundamental rights which should be afforded individuals in this third category, to include humane treatment; prohibitions against murder, torture, corporal punishment, mutilation, and collective punishment; and due process before imposing a sentence for penal offenses. Article 75 of AP I additionally states that "any person . . . detained . . . for actions related to the armed conflict shall be informed promptly of the reasons why these measures have been taken [and] . . . shall be released with minimal delay possible." *Id.*

> and, as such, covered by the Third Convention, a civilian covered by the Fourth Convention, or again, a member of the medical personnel of the armed forces who is covered by the First Convention. There is no intermediate status; nobody in enemy hands can be outside the law. We feel that this is a satisfactory solution - not only satisfying to the mind, but also, and above all, satisfactory from the humanitarian point of view.[108]

Second, the International Criminal Tribunal for the Former Yugoslavia has found that there "is no gap between the Third and the Fourth Geneva Conventions. If an individual is not entitled to the protections of the Third Convention as a prisoner of war (or of the First or Second Conventions) he or she necessarily falls within the ambit of Convention IV, provided that its article 4 requirements are satisfied."[109]

The United States disagrees with the international position that there are only two classes of individuals within an international armed conflict. The first reference to unlawful combatants under United States domestic law appears in the 1942 U.S. Supreme Court case *Ex Parte Quirin*.[110] This case pertained to German soldiers during World War II who infiltrated the Eastern United States in civilian dress for the purpose of committing sabotage to U.S. war industries and facilities.[111] The Court held that these soldiers were not lawful combatants under the Third Geneva Convention and were instead unlawful combatants not entitled to protections under the Geneva Conventions.[112] Following the September

---

[108] Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 4 cmt. 4, Aug. 12, 1949, 75 U.N.T.S. 287.

[109] Prosecutor v. Delalić, Mucić, Delić & Landžo, Case No. IT-96-21, Judgment, ¶ 271 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998); *see also* Prosecutor v. Tihomir Blaškić, Case No. IT-95-14-T, Judgment, ¶ 60 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 3, 2000) (holding that civilians are "persons who are not, or no longer, members of the armed forces").

[110] 317 U.S. 1 (1942).

[111] *Id.* at 2. The soldiers landed under cover of darkness in their uniforms but then buried their uniforms and supplies and proceeded with their mission in civilian dress.

[112] *See id.* at 30–31 ("By universal agreement and practice, the law of war draws a distinction between . . . lawful and unlawful combatants"); *see also id.* at 35 ("It has long been accepted practice by our military authorities to treat those who, during time of war, pass surreptitiously from enemy territory into our own, discarding their uniforms upon entry, for the commission of hostile acts involving destruction of life or property, as

11, 2001 attacks, President George W. Bush issued a White House memorandum stating that the U.S. government had determined that al-Qaeda terrorists and members of the Taliban captured during the course of the conflict did not meet the requirements of prisoners of war and were therefore not entitled to the protections of the Third Geneva Convention.[113]

The Congress has followed suit. The Military Commissions Act of 2006 uses the term "unlawful enemy combatant," which it defines as an individual who has engaged in or materially supported hostilities against the United States or its allies who is not a lawful enemy combatant.[114] A slightly different term is used in the 2009 amendment to the Military Commissions Act—"unprivileged enemy belligerent."[115] Although the term has changed slightly throughout the years, the current U.S. policy remains the same; specifically, that any individuals who engage in hostilities against the United States or its coalition partners and who do not fall under one of the delineated categories under the Third Geneva Convention are neither POWs nor civilians but members of a third category.[116] For the sake of clarity, this article will continue to refer to them as "unlawful combatants."

---

unlawful combatants punishable as such by military commission."). It is important to note, however, that the soldiers at issue in this case were privileged combatants who lost their status based on their conduct of taking off their uniforms for the purposes of committing sabotage. *Id*. at 21, 36. They were not civilians directly participating in hostilities nor were they non-state actors.

[113] THE WHITE HOUSE, HUMANE TREATMENT OF TALIBAN AND AL QAEDA DETAINEES (Feb. 7, 2002), *available at* http://www.pegc.us/archive/WhiteHouse/bushmemo20002 0207ed.pdf.

[114] Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2601.

[115] National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, § 1802, 123 Stat. 2575.

[116] *Id.* However, see also FM 27-10, *supra* note 33, which is at odds with the current policy:

> The enemy population is divided in war into two general classes:
>
> a. Persons entitled to treatment as prisoners of war upon capture, as defined in Article 4, GPW (par. 61).
>
> b. The civilian population (exclusive of those civilian persons listed in GPW, art. 4), who benefit to varying degrees from the provisions of GC (see chs. 5 and 6 herein). Persons in each of the foregoing categories have distinct rights, duties, and disabilities. Persons who are not members of the armed forces, as defined in Article 4, GPW, who bear arms or engage in other conduct hostile to

C. Classification of Cyberterrorists

As discussed in Part II, this article proposes the following definition of cyberterrorist: a non-state actor who uses cyber assets to directly participate in hostilities. It is assuredly possible for a state actor to commit an act of cyberterror and thereby become a privileged combatant under the Third Geneva Convention. For example, if the United States were to engage in an international armed conflict with Libya, it is not beyond the realm of possibility that a member of the Libyan armed forces could launch a cyber attack or threaten to launch a cyber attack on the Washington, D.C. power grid for the purpose of spreading terror among the civilian population. However, in the context of the current War on Terror, cyberterrorists are more likely to be non-state actors.

A non-state actor who engages in cyberterrorism will in most cases be an unlawful combatant. The very nature of cyberterrorism is that it consists of acts that can be carried out clandestinely in sealed rooms in front of computer screens. Additionally, acts of cyberterrorism can create widespread damage with significantly less resources than those required to conduct a traditional kinetic attack, which makes cyber attacks more attractive to groups with less funds and limited organization.[117]

When examining the framework of terrorist groups such as al-Qaeda or its numerous sympathetic off-shoots, the question must necessarily be raised as to whether the very organization of these groups places their members under the umbrella of privileges guaranteed by the Third Geneva Convention. The Third Geneva Convention creates a category of lawful combatants for members of organized groups that meet the additional four criteria of carrying arms openly, wearing a distinct sign or emblem, operating under a chain of command, and following the rules of armed conflict.[118] An organized terrorist organization may conceivably create lawful combatants if it satisfies those four criteria. However, this is unlikely when discussing cyberterrorism. The virtual nature of cyber activities does not allow for the open carrying of arms or wearing of

---

> the enemy thereby deprive themselves of many of the privileges attaching to the members of the civilian population.

Id.

[117] Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011 (2010).

[118] GC III, *supra* note 15.

distinctive signs or emblems to distinguish these actors from protected civilians.[119]

The *Tallinn Manual* agrees that civilians who take a direct part in hostilities via cyber activity are "unprivileged belligerents." Significantly, there is no minority view among the international group of experts regarding the classification of this group of cyber actors. All members agreed that these unlawful combatants "enjoy no combatant immunity and are not entitled to prisoner of war status."[120]

The experts concluded that unlawful combatants who engage in cyber acts are subject to prosecution under domestic law even if the acts would be lawful when committed by a lawful combatant under the law of armed conflict. The commentary within the *Tallinn Manual* makes note that many cyber activities, to include certain types of hacking, have been criminalized under domestic law. The analysis, however, stops short of addressing alternative means of addressing these activities in an international legal framework.[121]

D. Lawful Actions Available to U.S. Armed Forces Against Cyberterrorists

The United States remains in an international armed conflict with al-Qaeda, as well as the Taliban and associated forces, to include ISIL.[122] As a result, as articulated by Harold Hongju Koh, Legal Adviser, U.S. Department of State, at the 2010 Annual Meeting of the American Society of International Law, the United States may use force consistent with its inherent right to self-defense under international law during the pendency of the international armed conflict.[123]

---

[119] TALLINN MANUAL, *supra* note 12, at 96–101.
[120] *Id.* at 98.
[121] *Id.* at 96–101.
[122] *See, e.g.*, 2010 NATIONAL STRATEGIC STRATEGY, *supra* note 1 (The United States is still in an international armed conflict with the Taliban, al-Qaeda, and associated forces.); Stephen W. Preston, General Counsel of the Department of Defense, Remarks on the Legal Framework for the United States' Use of Force Since 9/11 (Apr. 10, 2015) (ISIL is an associated force of al-Qaeda.).
[123] Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Remarks at the Annual Meeting of the American Society of International Law (Mar. 25, 2010) *available at* http://www.state.gov/s/l/releases/remarks/139119.htm.

Because the War on Terror is an international armed conflict made up of a dispersed group of non-state actors and the nature of the conflict makes it more conducive to clandestine acts of terror, commanders are likely to encounter acts of cyberterrorism during the course of this conflict. Once an individual is identified as a cyberterrorist directly participating in hostilities and classified as an unlawful combatant, there are two legally viable options available to commanders: target (use lethal force) or capture and detain. However, these options must be separated into two distinct categories: legally viable actions under LOAC and legally viable actions under U.S. policy.

1. Legally Viable Actions under LOAC

Civilians who directly participate in hostilities during an ongoing international or non-international armed conflict may be lawfully targeted under LOAC. There was a consensus among the international group of experts regarding what actions can be taken against a civilian directly participating in cyber hostilities. In the commentary to Rule 35 of the *Tallinn Manual*, paragraph 3 states:

> An act of direct participation in hostilities by civilians renders them liable to be attacked, by cyber or other lawful means. Additionally, harm to direct participants is not considered when assessing the proportionality of an attack . . . or determining the precautions that must be taken to avoid harming civilians during military operations.[124]

A more complicated question is what to do about attacks from non-state actors on behalf of a state that has not yet been declared belligerent. Consider the case of a hypothetical Iranian computer student who is outraged by the U.S.'s alleged involvement in the Stuxnet worm that crippled Iranian nuclear facilities.[125] In retaliation, on behalf of his state but without state sanction, this student creates a logic bomb designed to shut down the New York City power grid. Could this Iranian student be

---

[124] TALLINN MANUAL, *supra* note 12, at 119. The omitted language pertains to a reference to Rule 51 of the *Tallinn Manual* that addresses proportionality.

[125] *See* The Frontline, *U.S. Identified as Stuxnet Perpetrator with Obama's Backing*, V3 (June 1, 2012), http://www.v3.co.uk/v3-uk/the-frontline-blog/2181770/identified-stuxnet-perpetrator-obamas-backing.

targeted by U.S. armed forces? The answer is not clear-cut. The act would not constitute direct participation in hostilities because it did not take place during an international armed conflict. However, the act may rise to the level of a cyberattack that would open the doors to a state's right of self-defense under Article 51 of the United Nations Charter.[126] If the act is considered an armed attack, targeting may be authorized.[127]

A commander may alternatively choose to capture and detain an identified cyberterrorist. Because the cyberterrorist would be classified as an unlawful combatant, the treatment of that cyberterrorist is not bound by the protections found in the Third Geneva Convention or by the protections found in the Fourth Geneva Convention.[128]

2. Legally Viable Actions under U.S. Policy

Although the options to either target or capture and detain cyberterrorists are available to U.S. armed forces, they are restricted pursuant to U.S. policy. On May 23, 2013, President Barack Obama presented the current U.S. policy on counterterrorism during an address at National Defense University, which was codified as Presidential Policy Guidance.[129] The President reaffirmed the U.S. position that the country is "at war with al Qaeda, the Taliban, and their associated forces" and that the use of force is therefore justified under international law. As a matter of policy, however, use of force is restricted in several ways.

---

[126] U.N. Charter art. 51.

[127] *Id.*

[128] *See, e.g.*, GC III, *supra* note 15; GC IV, *supra* note 15; AP I, *supra* note 14, art. 45(3) (stating that "[a]ny person who has taken part in hostilities, who is not entitled to prisoner-of-war status and who does not benefit from more favourable treatment in accordance with the Fourth Convention shall have the right at all times to the protection of Article 75 of this Protocol."). Additional Protocol I, Article 75 lists "fundamental guarantees." AP I, *supra* note 14, art. 75.

[129] May 23 Speech on Counterterrorism, *supra* note 80. The Fact Sheet contains the following link to the full text of the Presidential Policy Guidance and is available at http://www.whitehouse.gov/sites/default/files/uploads/2013.05.23_fact_sheet_on_ppg.pdf.

a. Preference for Capture

The President stated that it is the policy of the United States to "not . . . use lethal force when it is feasible to capture a terrorist suspect, because capturing a terrorist offers the best opportunity to gather meaningful intelligence and to mitigate and disrupt terrorist plots." He qualified this position with the supposition that the operation must first be conducted in accordance with "all applicable law." If capture of a terrorist is not feasible, lethal force is authorized but only under restraints that are still more restrictive than what is required under LOAC.[130]

b. Restraints on Use of Force

In accordance with the policy delineated in the May 23 speech, if capture of a terrorist is not feasible, U.S. forces may only use lethal force "to prevent or stop attacks against U.S. persons, and [when] . . . no other reasonable alternatives exist to address the threat effectively."[131] Using lethal force to prevent or stop attacks is analogous to using lethal force to engage a person committing a hostile act or demonstrating hostile intent excepting the qualifier that the attack or threatened attack must be against U.S. persons. The policy, however, places an additional restriction, not found in the SROE, that a determination must first be made that there are no reasonable alternatives to lethal force. On a conventional battlefield, there are few alternatives to prevent or stop an attack outside of either capture or lethal force, other than perhaps disarmament. In cyberspace, however, alternatives could include disabling a cyberterrorist's capabilities by, for example, destroying or disrupting his cyber assets or access to those assets.

The current U.S. policy places additional restraints on actions against terrorists located outside of the area of hostilities. If an identified terrorist is located outside of "areas of active hostilities," the policy states that lethal force may only be used if the following preconditions are met:

> (1) the terrorist poses a "continuing, imminent threat to U.S. persons;" (2) there is "near certainty" that the terrorist is present; (3) there is "near certainty that non-combatants will not be injured or killed;" (4) "capture is

[130] May 23 Speech on Counterterrorism, *supra* note 81.
[131] *Id.*

> not feasible at the time of the operation;" (5) the government authorities in the country where the terrorist is located "cannot or will not effectively address the threat;" and (6) "no other reasonable alternatives exist."[132]

Returning to the hypothetical LulzKhat, under international law, he could be lawfully targeted with lethal force as a cyberterrorist. Under U.S. policy, however, lethal force could be used only if the capture of LulzKhat was not feasible and the other preconditions were met. The precondition that would likely prevent the greatest obstacle to the use of lethal force is the requirement to assess reasonable alternatives to stop the threat. As discussed above, a cyberterrorist can be effectively disarmed and rendered incapable of posing a further threat by disabling his cyber assets or otherwise preventing his access to those assets. If computer specialists onboard the USS *Bonhomme Richard* are able to isolate and remove the malware, under U.S. policy, lethal force could not be contemplated. United States forces could still capture and detain LulzKhat; and because he is an unlawful combatant, his treatment would not be bound by the protections found in the Third Geneva Convention nor by the protections found in the Fourth Geneva Convention.

IV. Conclusion

In an open hearing of the Senate's intelligence committee in early 2012, Director of National Intelligence James Clapper stated in reference to cyber attacks that non-state actors are increasingly gaining in prominence, and in fact already have "easy access to potentially disruptive and even lethal technology."[133] This warning was echoed by then U.S. Secretary of Defense Leon Panetta in a 2012 address on cybersecurity:

> Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st Century. And yet, with these possibilities, also come new perils and new dangers. The Internet is open. It's highly

---

[132] *Id.*

[133] J. Nicholas Hoover, *Cyber Attacks Becoming Top Terror Threat, FBI Says*, INFO. WK., Feb. 1, 2012, *available at* http://www.informationweek.com/security/risk-management/cyber-attacks-becoming-top-terror-threat-fbi-says/d/d-id/1102582.

> accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. But the even greater danger—the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.[134]

For these reasons, it is more important than ever to pierce the "penumbral mist" that surrounds the applicability of international law to cyber war, specifically as it pertains to the identification and classification of non-state actors that engage in cyber hostilities.[135]

Although cyber war resists traditional classification, cyberspace is the terrain of modern warfare. The use of cyber technology, which can inflict high amounts of damage using significantly less resources and manpower than traditional kinetic warfare, has created an increasing amount of opportunities for civilians to participate in hostilities in the course of international armed conflict.[136]

As the United States continues to engage extremist groups in the ongoing international armed conflict against al-Qaeda, the Taliban, and associated terrorist organizations, to include ISIL, there is a growing emphasis in combating against cyber attacks.[137] What has been termed "The War on Terror" has no definable battlefield borders but instead is a global asymmetric campaign. Cyberterrorists operate on a global scale to conduct attacks or threats of attacks with the intent to spread terror to achieve their strategic goals.[138] Identifying and classifying individuals who are engaged in acts of cyberterrorism are the first steps in being able to determine the legal courses of action available to members of the U.S. armed forces in combating cyberterrorists. United States military doctrine to date does not provide the tools necessary to successfully identify and classify non-state actors engaged in acts of cyberterrorism.

---

[134] Leon E. Panetta, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012).
[135] Schmitt, *supra* note 13, at 176.
[136] Wenger & Mason, *supra* note 9, at 838.
[137] *Id.* at 847; *see also* Cha, *supra* note 10, at 400.
[138] ARREGUIN-TOFT, *supra* note 11.

The *Tallinn Manual* provides the most clear-cut guidance on this issue but nonetheless leaves many questions unanswered.[139]

The intent of this article was to address those gaps as they pertain to the identification and classification of cyberterrorists. Cyberterrorists can be identified though an examination of their conduct and the intent behind their conduct using a direct participation in hostilities analysis. Under LOAC, cyberterrorists who directly participate in hostilities can, during the course of that participation, be lawfully targeted with lethal force. United States policy restricts the use of lethal force against terrorists, instead mandating that U.S. forces first assess the feasibility of capture. Under both LOAC and U.S. policy, however, because cyberterrorists are unlawful combatants, they do not qualify for the protections provided by the Third and Fourth Geneva Conventions. These individuals can therefore be detained without being afforded POW status and without receiving the accompanying rights and privileges POW status brings.

The United States and international community, through the Koh speech and *Tallinn Manual*, have appeared to reach a consensus on the applicability of international law to cyber warfare. However, just how that law is to be interpreted is still up for debate. Until such a time that a more thorough consensus is reached, the United States and its armed forces will have to pursue its military strategy as it pertains to cyber warfare within the mists of uncertainty.

---

[139] TALLINN MANUAL, *supra* note 12, at 115–16.