

---

---

# INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE



The Law of Armed Conflict's  
“Wicked” Problem:  
*Levée en Masse* in Cyber Warfare

*David Wallace*  
*Shane R. Reeves*

89 INT'L L. STUD. 646 (2013)

Volume 89

2013

---

---

## The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare

David Wallace  
Shane R. Reeves\*

*The defense of the nation, an insurrection of the people must be initiated. . . . There is absolutely no time for delay.*

Walther Rathenau, "A Dark Day" (1918)<sup>1</sup>

*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 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.*

U.S. Secretary of Defense Leon E. Panetta<sup>2</sup>

---

\* David Wallace is a Colonel in the United States Army and a Professor and the Deputy Head, Department of Law at the United States Military Academy, West Point, New York. Shane Reeves is a Major in the United States Army and an Assistant Professor at the United States Military Academy, West Point.

1. Michael Geyer, *People's War: The German Debate About a Levée en Masse in October 1918*, in *THE PEOPLE IN ARMS: MILITARY MYTH AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION* 124 (Daniel Moran & Arthur Waldron eds., 2003).

2. Leon E. Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012).

## I. INTRODUCTION

Attempting to categorize and label a contemporary armed conflict is a complicated task. Not restricted to “hot battlefields,”<sup>3</sup> and an amalgamation of asymmetric and conventional tactics, modern wars escape traditional conflict classifications.<sup>4</sup> International or non-international armed conflict and irregular or conventional war are no longer workable distinctions as conflict participants now engage “along a broad spectrum of operations and lethality.”<sup>5</sup> These aptly titled “hybrid armed conflicts”<sup>6</sup> create an unpredictable operational environment<sup>7</sup> that is exacerbated by ever-increasing civilian participation in hostilities<sup>8</sup> and the emergence of new technologies.<sup>9</sup> Prognostica-

---

3. “Hot battlefields” is a term used to reference geographically contained conflicts. For example, Afghanistan, or, until recently, Iraq would be construed as a hot battlefield. See, e.g., Ashley S. Deeks, *Pakistan’s Sovereignty and the Killing of Osama Bin Laden*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS, <http://www.asil.org/insights110505.cfm> (last visited Feb. 9, 2012) (“the most controversial aspect . . . is the U.S. argument that this conflict can and does extend beyond the “hot battlefield” of Afghanistan to wherever members of al Qaeda are found”).

4. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 8 (2010) [hereinafter QDR] (discussing the difficulty in categorizing contemporary conflicts).

5. See Robert Gates, U.S. Secretary of Defense, Remarks at Maxwell Air Force Base, Alabama (Apr. 15, 2009), <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4403> (noting “black and white distinction[s] between irregular war and conventional war is an outdated model”); see also QDR, *supra* note 4, at 8.

6. See QDR, *supra* note 4, at 8 (stating “[t]he term ‘hybrid’ has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict.”); see also Shane R. Reeves & Robert E. Barnsby, *The New Griffin of International Law: Hybrid Armed Conflicts*, HARVARD INTERNATIONAL REVIEW, Winter 2013, at 16–18, available at <http://hir.harvard.edu/mobile-might/the-new-griffin-of-war> (discussing the international legal challenges presented by hybrid warfare).

7. See U.S. Department of the Army, TRADOC Pam. 525-3-1, The United States Army Operating Concept 2016–28, ¶ 2-2(a) (2010) [hereinafter CAPSTONE CONCEPT].

8. See INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 7 (Nils Melzer ed., 2009) [hereinafter ICRC Interpretive Guidance], available at <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf> (stating “there is little reason to believe that the current trend towards increased civilian participation in hostilities will weaken over time”).

9. See QDR, *supra* note 4, at 80.

tors believe this trend towards ambiguity in armed conflict is becoming the norm rather than the exception.<sup>10</sup> Perhaps no domain in modern warfare more starkly validates this prediction than cyberspace.<sup>11</sup>

Applying the law of armed conflict, as currently constructed, in this environment is “highly problematic”<sup>12</sup> as legal obligations are almost impossible to discern.<sup>13</sup> Recognizing this problem, the NATO Cooperative Cyber Defence Centre of Excellence recently enlisted an international group of experts, led by Professor Michael Schmitt of the Naval War College, to draft the *Tallinn Manual on the International Law Applicable to Cyber Warfare* “to help government’s deal with the international legal implications of cyber operations.”<sup>14</sup> In hopes of providing clarity for those governments, this recently published work attempts to explain how the existing law of armed conflict

---

10. See CAPSTONE CONCEPT *supra* note 7, ¶ 2-2(a); QDR, *supra* note 4, at iii.

11. CAPSTONE CONCEPT *supra* note 7, ¶ 5-7(a) (stating “[a] critical enabler for virtually all elements of national and military power, cyberspace has become an increasingly contested domain.”). The overarching importance of cyberspace in modern warfare cannot be overstated. See e.g., RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 69 (2010); Stephen W. Korn & Joshua E. Kastenberg, *Georgia’s Cyber Left Hook*, PARAMETERS, Winter 2008–09, at 60 (discussing the desperate actions of the Georgian government after it found itself unable to communicate through the Internet during the 2008 Georgian-Russian conflict); William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, 11 BALTIC SECURITY & DEFENSE REVIEW 4 (2009) (discussing the adverse effects of the 2007 cyber attack on Estonia); David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, NEW YORK TIMES, Feb. 18, 2013, at A1 (describing a series of aggressive cyber attacks carried out by Unit 61398, a Chinese military unit, against various U.S. government agencies and corporations and the potential responses).

12. Korn & Kastenberg *supra* note 11, at 71.

13. Stephen Daggett, Congressional Research Service, R41250, Quadrennial Defense Review 2010: Overview and Implications for National Security Planning 2 (2010); see also Nils Melzer, *Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC’s Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 831, 833 (2010) (discussing the difficulties in contemporary armed conflicts due to the “blurring of the traditional distinctions and categories upon which the normative edifice of IHL has been built”).

14. See, e.g., *Manual Examines How International Law Applies to Cyberspace*, IT WORLD, (Sept. 3, 2012), <http://www.itworld.com/legal/293042/manual-examines-how-international-law-applies-cyberwarfare> (noting that The Cooperative Cyber Defense Center of Excellence, which “assists NATO with technical and legal issues associated with cyber warfare related issues,” created the *Tallinn Manual* to address a variety of cyber legal issues).

generally regulates cyber warfare.<sup>15</sup> However, when specific provisions of the law of armed conflict are applied in cyber warfare, it is apparent that generalities do not address the truly “wicked” nature of the problem.<sup>16</sup> One particular example—trying to reconcile the concept of *levée en masse* with the “cyber conflicts between nations and ad hoc assemblages”—illustrates how ill-suited, and often impractical, the existing law of armed conflict can be when applied in the cyber context.<sup>17</sup>

To support this proposition, this article will begin with a brief discussion on the history of a *levée en masse*. An explanation of how the law of armed conflict defines and characterizes the individual battlefield status associated with *levée en masse* will follow. The article will then explore the unique aspects of hostilities in cyberspace and delve into the impracticality of applying the concept of *levée en masse* in the context of cyber warfare. It will conclude with specific recommendations in terms of the reconceptualising of a *levée en masse* in cyber warfare and a hope that, by focusing on this nuanced provision of the law of armed conflict, a broader discussion will ensue.

## II. PEOPLE IN ARMS—HISTORY AND BACKGROUND ON THE LEVÉE EN MASSE

A distinct type of resistance movement in warfare has been the collective uprising limited to the actual period of the invasion of a territory—a *levée en masse*.<sup>18</sup> Having acquired something of a mythical status in the history of war,<sup>19</sup> the underlying concept of a *levée en masse* is simply that during the initial invasion, the civilian population of unoccupied territory can spontaneously take up arms against the invading army in order to forestall an occupa-

---

15. The *Tallinn Manual* examines the “international law governing cyber warfare” and encompasses both *jus ad bellum* and the *jus in bello*. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael Schmitt ed., 2013).

16. “Wicked problems” are generally defined as extraordinarily complex and tricky issues that evade traditional solutions. *See generally* Horst W.J. Rittel & Melvin M. Webber, *Dilemmas in a General Theory of Planning*, 4 POLICY SCIENCES 155 (1973). Instead, novel and creative ideas are required to develop a workable answer as a definitive solution may never be possible. *Id.* at 162–63.

17. Korns & Kastenberg *supra* note 11, at 70.

18. KARMA NABULSI, TRADITIONS OF WAR: OCCUPATION, RESISTANCE, AND THE LAW 52 (2004).

19. *See* Karma Nabulsi, *Levée en Masse*, CRIMES OF WAR (Mar. 11, 2013), <http://www.crimesofwar.org/a-z-guide/levee-en-masse/> (stating “[t]he *levée en masse*, or mass uprising, has acquired something of a mythical status in the history of war.”).

tion.<sup>20</sup> Underpinning the revolutionary mobilization of a *levée en masse* is patriotic zeal coupled with the initiative of the citizen-soldier under emergency circumstances.<sup>21</sup> The *levée en masse* institutionalizes total war in the context of the defense of a nation,<sup>22</sup> with all members of the community having a role until the enemy had been repelled or defeated.<sup>23</sup> As both territorial occupation and spontaneity are defining characteristics, a *levée en masse* is a key legal classification of participants typically during an early and brief period of an armed conflict.

The law of armed conflict recognizes that a *levée en masse* occurs when inhabitants of a non-occupied territory, without time to form into a regular armed unit, spontaneously take up arms to resist an invading force.<sup>24</sup> *Levée en masse* participants are considered lawful combatants and are entitled to prisoner-of-war status if they carry arms openly and respect the laws and customs of warfare.<sup>25</sup> Endowing *levée en masse* participants with lawful combatant status recognizes—and reinforces—the belief that “[t]he first duty of a citizen is to defend his country, and provided he does so loyally he should not be treated as a marauder or criminal.”<sup>26</sup> The Lieber Code, the Brussels Declaration, the Hague Regulations, and the Third Geneva Convention all expressly encapsulate in positive legal provisions the special status given to *levée en masse* participants.<sup>27</sup>

---

20. YORAM DINSTEIN, *THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT* 42 (1st ed. 2004).

21. Dierk Walter, *Reluctant Reformers, Observant Disciples: The Prussian Military Reforms, 1807–1814*, in *WAR IN AN AGE OF REVOLUTION 1775–1815*, at 87, 87 (Roger Chickering & Stig Forster eds., 2010).

22. Scott Lytle, *Robespierre, Danton, and the Levée en Masse*, 30 *JOURNAL OF MODERN HISTORY* 325, 325 (1958).

23. Alan Forrest, *The French Revolution and the First Levée en Masse*, in *THE PEOPLE IN ARMS: MILITARY MYTHS AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION* 14 (Daniel Moran & Arthur Waldron eds., 2003).

24. Convention Relative to the Treatment of Prisoners of War art. 4(A)(6), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; GARY SOLIS, *THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 200–201*(2010)(citing Prosecutor v. Delalić, IT-96-21-T, Judgment, ¶ 268 (Int’l Crim. Trib. for the former Yugoslavia Nov 16, 1998)).

25. GC III, *supra* note 24, art. 4A(6).

26. MORRIS GREENSPAN, *THE MODERN LAW OF LAND WARFARE* 62 (1959).

27. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 2 *CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: PRACTICE* 2545–50, §§49–80 (2005) [hereinafter *PRACTICE*] (discussing the historical acceptance of the concept of *levée en masse*).

The concept of a *levée en masse* is deeply rooted in history with its origins firmly planted in the French Revolution.<sup>28</sup> The French Revolution marked a dramatic shift from dynastic warfare between kings to mass participation of the populace as citizens took up arms to defend their national soil.<sup>29</sup> Based on a principle of the nation in arms, the armies of the French Revolution represented a significant departure from centuries of tradition regarding military organization for warfare.<sup>30</sup> On August 23, 1793, the National Convention under the leadership of its Committee of Public Safety, in one of the most celebrated decrees of the French Revolution,<sup>31</sup> issued the following statement:

From this moment until that in which every enemy has been driven from the territory of the Republic, every Frenchman is permanently requisitioned for service with the armies. The young men shall fight; married men will manufacture weapons and transport stores; women shall make tents and nurse in the hospitals; children shall turn old linen into lint; the old men shall report to the public square to raise the courage of the warriors and preach the unity of the Republic and hatred against the kings.<sup>32</sup>

Accordingly, military units were formed on a territorial basis. In September 1793, recruiting under the *levée en masse* decree provided over 450,000 men for the French armies.<sup>33</sup> On October 15 of that year, the concept of *levée en masse* was validated at the Battle of Wattignies as a viable form of warfare when the French citizen-army successfully beat back invading regular military units from Austria.<sup>34</sup>

The French, though formalizing the term and concept, are by no means alone in using a *levée en masse*; history is replete with other examples. The

---

28. Emily Crawford, *Levée en Masse—A Nineteenth Century Concept in a Twenty-First Century World* 3 (Sydney Law School, Legal Studies Research Paper No. 11/31, May 2001), available at <http://ssrn.com/abstract=1851947> (noting that the concept originated with the French Revolution of 1789).

29. See Audrey Kurth Cronin, *Cyber-Mobilization: The New Levée en Masse*, PARAMETERS, Summer 2006, at 77, 77–78.

30. GUNTHER E. ROTHENBERG, *THE ART OF WARFARE IN THE AGE OF NAPOLEON* 95 (1980).

31. *Id.* at 100.

32. Lytle, *supra* note 22, at 325.

33. ROTHENBERG, *supra* note 30, at 100–110.

34. SOLIS, *supra* note 24, at 200.

Prussian *Erhebung*, or uprising, fueled the War of Liberation in 1813<sup>35</sup> as Prussian citizens, displaying patriotic feelings and a popular willingness to accept sacrifice, flocked to the colors to throw off the French yoke.<sup>36</sup> In 1864, during the United States Civil War, 257 cadets from the Virginia Military Institute formed a *levée en masse* to fight the approaching Union forces at the Battle of New Market.<sup>37</sup> In the closing months of World War I, a significant debate arose among both the German military and national public about the possibility of “going French” and waging a people’s war—a *volkskrieg*—against the allies.<sup>38</sup> For a variety of political, military and practical reasons, the Germans ultimately decided not to use a *levée en masse* to defend the “fatherland.”<sup>39</sup>

During World War II, in response to the German invasion of the Soviet Union (Operation Barbarossa), the Soviet’s placed “[n]early all inhabitants of the country from teenagers to the elderly . . . on call for either labor or military duty, and the distinctions between military and civilian life were once again erased.”<sup>40</sup> Professor Gary Solis, in his award winning book on the law of armed conflict, provides a compelling account of a *levée en masse* on Wake Island. He states, in part, as follows:

On December 24, 1941, two weeks after Pearl Harbor, U.S.-held Wake Island fell to invading Japanese forces. More than eleven hundred American civilian construction workers were among the island’s population. ‘More than sixty civilians are known to have taken part in the ground fighting and their valor—if not their combat skills—equaled that of the servicemen.’ One hundred twenty-four Americans died before Wake Island was forced to surrender. Seventy-five of the dead were civilians who manned shore batteries and heavy machine guns, held defensive positions and, when Japanese infantry landed, fought in counterattacks.<sup>41</sup>

In the aftermath of the Balkans War, the International Criminal Tribunal for the former Yugoslavia examined the question of whether a *levée en masse*

---

35. Daniel Moran, *Arms and the Concert: The Nations in Arms and the Dilemmas of German Liberalism*, in THE PEOPLE IN ARMS: MILITARY MYTHS AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION 52 (Daniel Moran & Arthur Waldron eds., 2003).

36. See Walter, *supra* note 21, at 90.

37. See SOLIS, *supra* note 24, at 200.

38. Geyer, *supra* note 1, at 124-25.

39. *Id.* at 124-58.

40. Mark Von Hagen, *People’s War: The German Debate about a Levée en Masse in October 1918*, in THE PEOPLE IN ARMS, *supra* note 35, at 187-88.

41. See Solis, *supra* note 24, at 200.

existed during a portion of the conflict. Evidencing its contemporary relevance, the Trial Chamber concluded that, for a brief period of time, the situation in and around Srebrenica in 1992 was characterized as a *levée en masse*.<sup>42</sup> More recently, in the 2008 armed conflict between Russia and Georgia over the autonomous and *de jure* demilitarized region known as South Ossetia,<sup>43</sup> the *New York Times* reported, in part, that:

As swaths of the country fell before Russian troops, it was not only the army that rose in its defense but also regular citizens . . . . [Two young Georgian men] hoped to join the fight . . . despite the fact neither had served in the military . . . . [They were] part of a group of dozen civilians, some in camouflage and some wearing bullet-proof vests, who said they were there to defend the city from Russian attack. . . . “Many of them now think it is the last chance to defend their homeland.” Ms. Lagidze said. “It comes from the knowledge that the army is not enough and every man is valuable.”<sup>44</sup>

---

42. Prosecutor v. Naser Orić, IT-03-68-T, Judgment, ¶¶ 135–36 (Int’l Crim. Trib. for the former Yugoslavia June 30, 2006). Those paragraphs provide as follows:

135. From its inception, the [Army of Bosnia and Herzegovina] sought to provide its members with means of identification such as uniforms, badges and insignia. In the Srebrenica area, however, with the exception of the members of the 16th East Bosnian Muslim Brigade (“16th Muslim Brigade”) led by Nurif Rizvanović, very few individuals possessed a complete uniform in 1992 and 1993. Before and after the arrival of this brigade in the area in early August 1992, most Bosnian Muslim fighters wore makeshift or parts of [Yugoslav People’s Army] uniforms. To make up for the lack of adequate clothing, civilians also sometimes wore parts of uniforms. There is evidence indicating that during some attacks, fighters wore coloured ribbons around their heads or arms for identification purposes amongst themselves. Apart from these disparate uniforms and ribbons, fighters did not wear fixed distinctive emblems recognizable at a distance.

136. The Trial Chamber comes to the conclusion that while the situation in Srebrenica may be characterized as a *levée en masse* at the time of the Serb takeover and immediately thereafter in April and early May 1992, the concept by definition excludes its application to long-term situations. Given the circumstances in the present case, the Trial Chamber does not find the term *levée en masse* to be an appropriate characterization of the organizational level of the Bosnian Muslim forces at the time and place relevant to the Indictment.

43. Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Tali harm & Lis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* 4 (2008), available at <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>.

44. SOLIS, *supra* note 24, at 200 (citing Nicholas Kulish & Michael Schwartz, *Sons Missing in Action, If Indeed They Found It*, NEW YORK TIMES, Aug. 13, 2008, at A14).

As it is extremely likely that in future conflicts there will again be civilian fighting forces that spontaneously form to defend their homeland, understanding both the historical context and legal definition of *levée en masse* is important. The concept of *levée en masse* remains a viable contemporary combatant status as various modern examples, most notably in the Balkans War and the Russian invasion of Georgia, clearly illustrate. Many military manuals and legal scholars are cognizant of the historical relevance and modern importance of the concept and continue to stress the validity of delineating *levée en masse* participants as combatants under the law of armed conflict.<sup>45</sup>

### III. THE LAW OF ARMED CONFLICT AND LEVÉE EN MASSE: RECOGNIZING AND REGULATING THE REALITIES OF WAR

A *levée en masse* is a unique and limited battlefield categorization available only during a portion of a declared war or international armed conflict.<sup>46</sup> The Third Geneva Convention of 1949 explicitly entitles participants of a *levée en masse*, upon capture, to prisoner-of-war status.<sup>47</sup> Qualifying for prisoner-of-war status means an individual may gain combatant status,<sup>48</sup> in contrast to

---

45. See generally PRACTICE, *supra* note 27, at 2546–50.

46. In the four 1949 Geneva Conventions, Common Article 2 states, in part, that “the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.” See, e.g., GC III, *supra* note 24, art. 2. Additionally, “[t]he Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.” *Id.* Thus, the Third Geneva Convention, including provisions concerning *levée en masse*, is triggered in the event of an international armed conflict, declaration of war, or occupation. *Id.* *Levée en masse* as a status does not apply during a non-international armed conflict as it is not provided for in Common Article 3 of the Geneva Conventions. *Id.*, art. 3; TALLINN MANUAL, *supra* note 15, at 102 (noting that a *levée en masse* does “not apply to non-international armed conflict”).

47. See GC III, *supra* note 24, art. 4(A)(6).

48. “Combatants are generally defined as anyone engaging in hostilities in an armed conflict on behalf of a party to the conflict” and fall “under the definition given in Geneva Convention III for those entitled to Prisoner of War status.” INTERNATIONAL & OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL’S LEGAL CENTER & SCHOOL, U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 134 (2010)[hereinafter DESKBOOK]. Article 4(A) of the Third Geneva Convention lists four categories of combatant. See GC III, *supra* note 24, art. 4(A)(1)–(3), (6). Article 4(A)(6), one of the explicit combatant categories, defines a *levée en masse* as: “Inhabitants of a non-occupied territory,

being defined as an unlawful combatant<sup>49</sup> or civilian.<sup>50</sup> Combatant status, which only exists in international armed conflicts and declared wars,<sup>51</sup> allows *levée en masse* participants to kill and wound without penalty, provided the privilege is not abused by unlawful battlefield acts.<sup>52</sup> As combatants, *levée en masse* participants are allowed to be lawfully attacked,<sup>53</sup> and as noted above,

---

who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.” More generally, combatants fall into two alternative categories: (1) members of the armed forces of a belligerent party (except medical and religious personnel) even if their specific task is not linked to active hostilities; and (2) any other person taking an active part in hostilities. DINSTEIN, *supra* note 20, at 27.

49. The law of armed conflict does not use the term “unlawful combatant” or “unprivileged belligerent.” However, these terms have become workable references to those who engage in combat without meeting the combatant criteria listed in Article 4 of the Third Geneva Convention. *See generally* SOLIS, *supra* note 24, at 206–11 (discussing the history of the terms, criticism of the concept and the negative consequences of being an unlawful combatant); DESKBOOK, *supra* note 48, at 96–97.

50. Despite the obvious significance of distinguishing between combatants and civilians on the battlefield, the Geneva Conventions do not define the term “civilians.” However, the *Commentary* to Additional Protocol I states that “the principle protection of the civilian population is inseparable from the principle of distinction which should be made between military and civilian persons,” therefore “it is essential to have a clear definition of each of these categories.” COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 610 (Yves Sandoz et al. eds., 1987). As a result, Additional Protocol I goes on to specifically define a civilian as “any person who does not belong to one of the categories referred to in Article 4(A)(1), (2), (3) and (6) of the Third Geneva Convention and in Article 43 of this Protocol.” Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict art. 50(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. Those listed in Article 4(4) and (5) (examples include journalist and others that accompany the armed force) maintain their civilian status, but are afforded the special status as a prisoner of war if captured.

It is important to note that the United States has not ratified Additional Protocol I, but finds many portions reflect customary international law. *See generally* Michael J. Matheson, *Remarks on the United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 419 (1987).

51. *See* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: RULES 11–12, Rule 3 (2005).

51. *See* GREENSPAN, *supra* note 26, at 3.

52. SOLIS, *supra* note 24, at 42.

53. A.P.V. ROGERS, LAW ON THE BATTLEFIELD 8 (2d ed. 2004).

afforded prisoner-of-war status upon capture.<sup>54</sup> However, “[t]he permissible window of opportunity for the raising of and participation in a *levée* is extremely narrow.”<sup>55</sup> The *Commentary* to the Third Geneva Convention acknowledges that a *levée en masse* can only exist for a short period of time as it is a spontaneous uprising and will eventually take on structure or no longer be in unoccupied territory.<sup>56</sup> Thus, if the *levée en masse* continues beyond the initial invasion, “the authority commanding the inhabitants who have taken up arms, or the authority to which they profess allegiance, must either replace them by sending regular units, or must incorporate them in its regular forces.”<sup>57</sup>

Recognizing the temporal nature of a *levée en masse*, participants receive combatant status under relaxed conditions and are exempt from two of the four conditions required of other irregular troops.<sup>58</sup> These other irregular troops, whether members of militia, other volunteer corps or those of organized resistance belonging to a party to a conflict, may be considered combatants and receive the resultant privileges, provided they fulfill the following four conditions:

- (a) that of being commanded by a person responsible for his subordinates;
- (b) that of having a fixed distinctive sign recognizable at a distance;
- (c) that of carrying arms openly;
- (d) that of conducting their operation in accordance with the laws and customs of war.<sup>59</sup>

In contrast, *levée en masse* participants are neither required to be commanded by a person responsible for his subordinates nor wear a fixed dis-

---

54. See GC III, *supra* note 24, art. 4(A)(6). The United States law of land warfare field manual states that “[s]hould some inhabitants of a locality thus take part in its defense, it might be justifiable to treat all the males of military age as prisoners of war.” U.S. Department of the Army, FM 27-10, *The Law of Land Warfare* 28 (Change 1, 1976)[hereinafter FM 27-10]. The manual goes on to say that “[e]ven if inhabitants who formed the *levée en masse* lay down their arms and return to their normal activities” they may still be made prisoners of war. *Id.*

55. Crawford, *supra* note 28, at 13.

56. COMMENTARY, III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 68 (Jean S. Pictet ed., 1960)[hereinafter COMMENTARY, GC III].

57. *Id.* See also Crawford, *supra* note 28, at 13.

58. See GREENSPAN, *supra* note 26, at 62; GC III, *supra* note 23, art. 4(A)(2).

59. GC III, *supra* note 24, art. 4(A)(6).

tinctive sign to receive combatant status.<sup>60</sup> Given that a *levée en masse* is a spontaneous, unorganized movement<sup>61</sup> acting under emergency conditions to desperately defend a nation,<sup>62</sup> it is understandable that the inhabitants of the territory will not have sufficient time to organize into units and have distinctive signs. Though justifiable, these relaxed combatant qualification standards significantly diminish the ability of an armed force fighting a *levée en masse* to distinguish between a civilian and a combatant.<sup>63</sup> Thus, “the requirement of carrying arms ‘openly’ is of special significance and has a more precise implication”<sup>64</sup> for both the *levée en masse* participants and their adversaries. For those fighting a *levée en masse*, the only distinguishing characteristic between a protected civilian and a combatant, and, therefore, who can be lawfully attacked, is the open carrying of arms. For *levée en masse* participants, “this requirement is in the interest of [the] combatants themselves who must be recognizable in order to qualify for treatment as prisoners of war.”<sup>65</sup> Recognizing both the realities of a *levée en masse* and the criticality of protecting civilians, the law of armed conflict places singular emphasis on the essential need for those choosing to participate in a spontaneous uprising to “carry arms visibly.”<sup>66</sup>

The concept of *levée en masse*, though narrower and more specific than originally espoused during the French Revolution, remains a contemporary combatant category.<sup>67</sup> Yet, as the law of armed conflict struggles to maintain the balance between military necessity and humanity in modern warfare,<sup>68</sup> particularly in cyber conflicts, the viability of a *levée en masse* must be questioned. A spontaneous uprising of a nation’s citizenry to defend the unoccupied portions of their territory is a far different paradigm than a cyber mobilization.

---

60. *See id.*; GREENSPAN, *supra* note 26, at 62. *See also* FM 27-10, *supra* note 54, at 28 (stating “[i]f the enemy approaches an area for the purpose of seizing it, the inhabitants, if they defend it, are entitled to the rights of regular combatants as a *levée en masse* although they wear no distinctive sign”).

61. GREENSPAN, *supra* note 26, at 62.

62. SOLIS, *supra* note 24, at 201.

63. *See supra* note 48 for membership criteria for a *levée en masse*.

64. COMMENTARY, GC III, *supra* note 56, at 68.

65. *Id.*

66. *Id.*

67. *See* Crawford, *supra* note 28, at 13 (stating “[a]s the concept of *levée en masse* has evolved and developed over the decades, it has become a far narrower concept than originally espoused during the French Revolution.”).

68. *See generally* Reeves & Barnsby, *supra* note 6, at 16–18 (discussing the difficulties of maintaining a balance between these countervailing interests in modern warfare).

IV. LEVÉE EN MASSE IN CYBER WARFARE:  
TECHNOLOGY MEETS TRADITION—AN ANALYSIS

The *Tallinn Manual*, the non-binding, yet authoritative interpretation of how the existing law of armed conflict applies to cyber warfare, addresses many critically important issues.<sup>69</sup> Of particular note is the *Manual's* Rule 27, which states that “in an international armed conflict, inhabitants of an unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status.”<sup>70</sup> In validating the notion of a cyber *levée en masse*, the international group of experts acknowledges the problematic nature of applying the concept to cyber warfare by highlighting various unanswered and troubling questions in the commentary to Rule 27.<sup>71</sup> Additionally, the experts were “divided as to whether the privileges associated with the *levée en masse* concept apply to a civilian population countering a massive cyber attack, the affects of which are comparable to those of a physical invasion by enemy forces.”<sup>72</sup> Unable to come to a consensus, a majority of the experts decided that the concept is only applicable when there is a physical invasion of national territory. Put differently, a cyber *levée en masse* is only possible when responding to a traditional invasion of territory by a conventional force.<sup>73</sup> It is not permitted in the face of an attack that consists only of cyber operations.

The *Tallinn Manual's* preservation, yet conservative treatment, of the concept of *levée en masse* is consistent with the belief that

[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.<sup>74</sup>

---

69. TALLINN MANUAL, *supra* note 15, at 1.

70. *Id.* at 102.

71. *See id.* at 102–03, cmt. to Rule 27 (discussing various problems with the concept of a cyber *levée en masse*).

72. *Id.* at 103.

73. *Id.*

74. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at*

Though this approach has merit, there is an equally compelling argument that it is critical to resolve the problems associated with extending the *levée en masse* concept to cyberspace. At the forefront of these problems is the inability to distinguish between a cyber *levée en masse* combatant and a protected civilian. As a *levée en masse* is a spontaneous uprising, inhabitants are expected to be participants in impulsively organized groups<sup>75</sup> that are only distinguishable as combatants by the open and visible carrying of arms.<sup>76</sup> There is no confusion as to what “arms” may mean in the context of a traditional *levée en masse*, as conventional weapons such as rifles, pistols and similar armaments are clearly contemplated.<sup>77</sup> *Levée en masse* participants, with no distinctive signs recognizable from a distance, are therefore expected to ostensibly carry traditionally recognized weapons since this is the only external display advertising their combatant status.<sup>78</sup>

This singular distinction requirement is not possible in a cyber war where the weapons are computers. Though a computer at times may be construed as a “weapon,”<sup>79</sup> simple possession cannot be interpreted to be indicative of combatant activity. As the *Tallinn Manual* notes, “even if [computers] qualify as weapons, the requirement to carry arms openly has little application in the cyber context,”<sup>80</sup> thus verifying that this most important of distinguishing characteristics is nonexistent. Without a visible weapon, there is no meaningful way to distinguish a theoretical cyber *levée en masse* from the civilian population.

The irrelevance of geography in cyberspace and the limited cyber expertise of a territory’s population both further contribute to this significant distinction problem.<sup>81</sup> Cyber warfare’s attractiveness is partially due to the abil-

---

[http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

75. GC III, *supra* note 24, art. 4(A)(6).

76. *See* COMMENTARY, GC III, *supra* note 56, at 67–68; *supra* text accompanying notes 61–66.

77. *See* COMMENTARY, GC III, *supra* note 56, at 61 (discussing the requirement of carrying arms openly, referring to weapons such as a hand grenade or a revolver).

78. *See id.* at 61, 67.

79. The *Tallinn Manual* defines a cyber weapon as “cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack.” TALLINN MANUAL, *supra* note 15, at 141–42.

80. *Id.* at 100.

81. *Id.*

ity of an individual to effectively organize a cyber campaign,<sup>82</sup> while remaining safely anonymous from an undisclosed location.<sup>83</sup> “Territory” is a non-factor in cyber warfare; the location of the cyber attacker, the digital infrastructure transmitting the attack and the target are widely dispersed and not bound by an occupied/unoccupied paradigm.<sup>84</sup> The territorial component that helps define a *levée en masse*, specifically that the uprising will remain restricted to “unoccupied territory,” thus does not comport with the realities of cyber warfare.<sup>85</sup> Further, “the means and expertise necessary to engage effectively in cyber operations may be relatively limited in the population,” eliminating the possibility of a mass uprising.<sup>86</sup> When comparing the historical narrative of a *levée en masse*—large numbers of armed citizens spontaneously coalescing in order to repel invaders—to the cyber version—technically skilled citizens discreetly using their computers from an undisclosed location to attack invaders<sup>87</sup>—the stark differences highlight the flaws in trying to apply the traditional concept in the cyber domain. A small dispersed group of citizens not limited to simply protecting unoccupied territory, but conducting cyber operations possibly deep inside enemy territory, is contrary to the conceptual underpinnings of a *levée en masse*.<sup>88</sup> Given the unlikely ability of a population to conduct a mass cyber uprising or for technically proficient citizens to limit a cyber attack to those forces “at the front,”

---

82. Korn & Kastenberg *supra* note 11, at 70.

83. See, e.g., Kelly Gables, *Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 57, 57 (2010) (discussing the unlimited reach of terrorist activity over the Internet).

84. Illustrating the irrelevance of geographic borders in cyberspace, author P.W. Singer noted when describing a Hezbollah cyber assault on Israel in 2006 that the attack “originally appeared to come from a small south Texas cable company, a suburban Virginia cable provider and web-hosting servers in Delhi, Montreal, Brooklyn, and New Jersey,” while in actuality “these all had actually been ‘hijacked’ by Hezbollah hackers.” P.W. SINGER, WIRED FOR WAR 264 (2009).

85. See Korn & Kastenberg *supra* note 11, at 70 (“Existing international laws of war are generally based on the notion of ‘borders’ in that these laws primarily govern conflicts between nation-states with recognized geographic boundaries. This construct is fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns.”).

86. TALLINN MANUAL, *supra* note 154, at 103.

87. *Id.* (discussing how a cyber *levée en masse* may theoretically form).

88. *Id.* (noting that historically, *levée en masse* did not “contemplate military operations deep inside enemy territory, it is questionable whether individuals launching cyber operations against enemy military objectives other than the invading forces can be considered a *levée en masse*”).

neither significant population participation nor geography can be considered distinguishing characteristics of a theoretical cyber *levée en masse*.

A cyber *levée en masse* is simply an unworkable notion whose continued viability increases the likelihood of greater indiscriminate targeting of the civilian population. Preserving a combatant category that lacks any distinctive indicators creates a murky environment<sup>89</sup> in which civilians may easily be mistaken for combatants.<sup>90</sup> One of the primary purposes of the law of armed conflict is to protect civilians,<sup>91</sup> as explicitly articulated in the principle of distinction,<sup>92</sup> thus “it is of the utmost importance that all feasible measures be taken to prevent the exposure of the civilian population to erroneous or arbitrary targeting.”<sup>93</sup> In contrast, a cyber *levée en masse* combatant category increases “confusion and uncertainty as to the distinction between legitimate military targets and persons protected against direct attack”<sup>94</sup> and therefore acts in direct opposition to this well-established principle. Whether due to the irresolvable distinction problem, or because of a complete dissimilarity between a traditional *levée en masse* and the cyber variant, it is untenable to maintain this combatant category in cyber warfare.

A more reasonable solution, which both enforces the principle of distinction and protects assemblages of cyber participants, is to require these groups to comply with a modified version of criteria required for other irregular troops, such as militias, volunteer corps or organized militia movements.<sup>95</sup> Because the existing criteria for traditional irregular troops to gain combatant status include “carrying arms openly,”<sup>96</sup> strict compliance with this requirement is not possible in any cyber context.<sup>97</sup> But unlike the concept of *levée en masse*, which places special significance on carrying arms

---

89. Distinguishing parties to the conflict in cyberspace is recognized as extraordinarily difficult. See Korns & Kastenber *supra* note 11, at 70.

90. See Melzer, *supra* note 13, at 833.

91. See ICRC Interpretive Guidance, *supra* note 8, at 4 (stating that “the protection of civilians is one of the main goals of international humanitarian law”).

92. The principle of distinction states that “in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives. . . .” AP I, *supra* note 50, art. 48.

93. ICRC Interpretive Guidance, *supra* note 8, at 7.

94. Melzer, *supra* note 13, at 833.

95. See GC III, *supra* note 24, art. 4(A)(2); text and accompanying notes 56-57 (listing the four criteria for irregular troops to gain combatant status).

96. See GC III, *supra* note 24, art. 4(A)(2)(c) (noting that the third cumulative condition for combatant status is “that of carrying arms openly”).

97. TALLINN MANUAL, *supra* note 15, at 100.

openly,<sup>98</sup> this requirement is not the only manner in which to recognize an irregular troop as a combatant. Carrying arms openly is of diminished importance in the irregular troop combatant category as other external signs, in particular “being commanded by a person”<sup>99</sup> and “having a fixed distinctive sign recognizable at a distance,” help distinguish these groups from civilians.<sup>100</sup> Though unfeasible in the context of a *levée en masse*,<sup>101</sup> eliminating this requirement as a qualification for an irregular cyber troop is a possibility due to the alternative distinguishing criteria.

Additionally, the remaining militia, volunteer corps and organized resistance movement membership criteria more accurately reflect current cyber war conditions than does the notion of a *levée en masse*. Limited technical expertise, coupled with the global scope of the cyber domain,<sup>102</sup> makes a spontaneous, geographically restricted mass cyber uprising an unrealistic, or, at best, extremely remote possibility.<sup>103</sup> A more likely scenario is a group of cyber-capable citizens, who possess the requisite technical expertise, inconspicuously organizing to engage an invading force in cyber warfare.<sup>104</sup> Organization of the cyber-capable citizens and the unrestricted use of cyberspace to affect the invading force are analogous to irregular troops being under command and allowed to operate “in or outside their own territory,

---

98. See COMMENTARY, GC III, *supra* note 56, at 67–68; *supra* text accompanying notes 62–64.

99. “The condition of being commanded by a person responsible for subordinates is best understood as an aspect of the requirement that the group be ‘organized.’” TALLINN MANUAL, *supra* note 15, at 98. As noted in the *Manual*, a group that is organized solely over the Internet will not qualify as an organized armed group as they will “have difficulty establishing that they are acting under a responsible commander” or “subject to an internal disciplinary system capable of enforcing compliance with the Law of Armed Conflict.” *Id.* Therefore, physical organization is required to gain combatant status. See *id.*

100. GC III, *supra* note 24, art. 4(A)(2)(a)(b).

101. The *Commentary* to the Third Geneva Convention, recognizing the critical importance of a *levée en masse* visibly carrying their weapons in order to be distinguished as combatants explains the difference between carrying arms “openly” and carrying them “visibly.” COMMENTARY, GC III, *supra* note 56, at 61.

102. TALLINN MANUAL, *supra* note 15, at 258–60 (defining cyberspace broadly and describing the Internet as “global”).

103. “At the core” of the *levée en masse* concept is “the notion of spontaneity and brevity.” Crawford, *supra* note 28, at 13. Gathering together those who have the technical expertise to conduct a concerted cyber attack will take effort and will unlikely comport to the understanding of “spontaneous.”

104. See Korns & Kastenbergh, *supra* note 11 at 70 (discussing the “the growing trend of cyber conflict between nations and ad hoc assemblages”).

even if [that] territory is occupied.”<sup>105</sup> Some may question the likelihood of a cyber group wearing “a fixed distinctive sign recognizable at a distance”;<sup>106</sup> however, since there are only a limited number of distinctive characteristics available in the cyber context, there is “no basis for deviating from” this general requirement if the group is to be afforded combatant immunity and prisoner-of-war status.<sup>107</sup> Similarly, as compliance with the law of armed conflict is a universal requirement for maintaining combatant status, this criterion obviously remains unchanged. For those individuals or loosely affiliated groups that choose to participate in cyber operations without meeting the modified membership criteria for a militia, volunteer corps or an organized resistance movement, they may be taking a direct part in hostilities.<sup>108</sup> In doing so, they risk divesting themselves of their civilian protections, thereby becoming subject to targeting and prosecution for belligerent acts.<sup>109</sup>

“When bombs and bullets fly, identification of warring parties is relatively easy; but not so for cyber activities,”<sup>110</sup> thus the need for greater clarity in defining a combatant in cyber warfare. Despite this necessity, the *Tallinn Manual* preserves the idea of a cyber *levée en masse*, thus maintaining a combatant status that is indistinguishable from the civilian population. In doing so, it ignores the contemporary realities of cyber warfare. This is dangerous and requires a workable alternative that provides the same opportunities for assemblages of cyber participants during the traditional period of a *levée en masse*. The membership criteria for the militia, volunteer corps or an organized resistance movement, modified for the cyber context, fills this need as it creates a combatant category for cyber capable citizens without the irresolvable issues of a *levée en masse*.

---

105. GC III, *supra* note 24, art. 4(A)(2).

106. *Id.*, art. 4(A)(2)(b).

107. Though there is “no basis for deviating from this general requirement for those engaged in cyber operations,” there are questions as to whether there are exceptions. *See generally* TALLINN MANUAL, *supra* note 15, at 99. Regardless of whether customary international law recognizes exceptions to this requirement in regards to a traditional militia, volunteer corps or organized resistance movements, in the context of cyber war this requirement has greater importance due to the limited number of distinctive characteristics available.

108. *See* AP I, *supra* note 50, art. 51(3).

109. *See generally* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 1 (2010) (discussing the consequences of a civilian taking a direct part in hostilities).

110. Korn & Kastenber *supra*, note 11, at 70.

## V. CONCLUSION &amp; RECOMMENDATION

*Levée en masse*, where “inhabitants of a non-occupied territory, on the approach of the enemy spontaneously take up arms to resist the invading forces, without having time to form themselves into regular armed units,” provides both prisoner-of-war protections and combatant immunity to individual participants if they “carry arms openly and respect the laws and customs of war.”<sup>111</sup> The requirements of spontaneous mass uprising, protecting non-occupied territory and “carrying arms openly” have special significance as these are essentially the only distinguishing characteristics of a *levée en masse*.<sup>112</sup> Because cyberspace is a borderless domain, where computers are the weapons and groups discreetly coalesce,<sup>113</sup> the concept of *levée en masse* becomes an unworkable anachronism whose application diminishes various protections afforded both civilians and conflict participants in armed conflicts.<sup>114</sup> Rather than forcibly applying a concept that is incongruous in this new domain, a more practical solution is to eliminate *levée en masse* as a combatant category in cyber conflicts and instead require all assemblages of cyber participants, either ad hoc or pre-existing, to generally comply with the criteria that define militias, volunteer corps or organized resistance movements.<sup>115</sup>

In contrast to *levée en masse*, this combatant category eliminates the importance of territorial occupation<sup>116</sup> and helps distinguish individual computer attacks from an organized cyber operation. Admittedly, this is not a perfect solution since computers are the exclusive tool used in cyberspace, and one of the qualifying conditions for militias, volunteer corps or orga-

---

111. GC III, *supra* note 24, art. 4(A)(6).

112. COMMENTARY, GC III, *supra* note 56, at 68.

113. QDR, *supra* note 4, at ix; Korns & Kastenberg *supra* note 11, at 70 (stating “international laws of war . . . are fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns”).

114. *See, e.g., supra* text accompanying notes 89–94 for a discussion on how applying the concept of *levée en masse* in a cyber conflict potentially increases indiscriminate targeting of civilians and confuses combatant status.

115. GC III, *supra* note 24, art. 4(A)(2). The following four conditions must be fulfilled to qualify for this provision: “(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war.”

116. *Id.*, art. 4(A)(2) (noting that members of this combatant category may operate “in or outside their own territory, even if [that] territory is occupied.”).

nized resistance movements includes the requirement to “carry arms openly.”<sup>117</sup> However, unlike a *levée en masse*, this category greatly diminishes the importance of “carry[ing] arms openly” by providing a variety of other criteria to help distinguish combatants from civilians.<sup>118</sup> If extended to include spontaneous cyber uprisings, the carrying arms openly requirement could be eliminated, while participants could remain in compliance with the principle of distinction through other means.<sup>119</sup> For those cyber assemblages not complying with the conditions that would categorize participants as members of a militia, volunteer corps or organized resistance movement as those apply to all other conflicts, individuals retain their civilian status until taking a direct part in hostilities.<sup>120</sup> Eliminating a possible *levée en masse* in cyber conflict and emphasizing the criteria, albeit slightly modified, defining militias, volunteer corps or organized resistance movements helps demarcate the line between a combatant and civilian in the ambiguous cyber war environment.

The impracticality of applying the concept of *levée en masse* in cyberspace, and the subsequent need to modify criteria for the irregular troop combat-

117. *Id.*, art. 4(A)(2)(c).

118. For example, a “fixed distinctive sign,” command structure and belonging to a party to the conflict. *Id.*, art. 4(A)(2)(c).

119. “In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives. . . .” AP I, *supra* note 50, art. 48. The distinction requirement also applies in non-international armed conflict. See Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II] (stating “civilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities”); SOLIS, *supra* note 24, at 254 (discussing the applicability of the principle of distinction in all conflicts); Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC ‘Direct Participation in Hostilities’ Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 641, 646 (2010) (“[c]ompliance with the distinction principle is required of all participants in warfare regardless of whether they fight for state armed forces or a non-State ‘organized armed group’”).

120. “Civilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities. AP I, *supra* note 50, art. 51(3); AP II, *supra* note 119, art. 13. There is much debate concerning what constitutes “a direct part in hostilities” in not only the cyber context, but in traditional forms of warfare. Compare ICRC Interpretive Guidance, *supra* note 8, at 5–6 (“The *Interpretive Guidance* provides a legal reading of the notion of ‘direct participation in hostilities’ with a view to strengthening the implementation of the principle distinction.”) with Watkin, *supra* note 119, at 641 and Schmitt, *supra* note 109, at 5 (criticizing the *Interpretive Guidance* recommendations). Though this particular issue is outside the purview of this paper, it again illustrates the difficulties faced when attempting to conform the existing law of armed conflict to cyber warfare.

ant category, highlights the immense challenge of regulating cyber warfare with the existing law of armed conflict. Cyberspace—“a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks”<sup>121</sup>—is quickly becoming a decisive battleground in warfare.<sup>122</sup> National armed forces, more specifically, technologically advanced militaries, are highly dependent upon their information networks for command and control, intelligence, logistics and weapon technology.<sup>123</sup> The result of this dependency is that “modern armed forces simply cannot conduct high-tempo, effective operations without . . . assured access to cyberspace.”<sup>124</sup> However, access to cyberspace is not limited to technologically advanced militaries as State actors with scarce resources, non-State armed groups or even individuals<sup>125</sup> are capable of cyber participation from almost any location.<sup>126</sup> Ease of access, widespread computer sophistication and cheap “hacker tools” allow this broad range of actors to create a staggering number of vulnerabilities for a cyber-reliant military.<sup>127</sup> Further, the anonymity and borderless nature of cyberspace incentivizes hostile actors to exploit these vulnerabilities,<sup>128</sup> making computer attacks an attractive method of warfare.<sup>129</sup> Cyber warfare, with all its concomitant legal issues is thus

---

121. See QDR, *supra* note 4, at 37.

122. *Id.*

123. *Id.*

124. *Id.*

125. See, e.g., Lee Ferran, *Former CIA Counter-Terror Chief: Al Qaeda Will Go Cyber*, (ABC Nightly News television broadcast Aug. 4, 2011), <http://abcnews.go.com/Blotter/cia-counter-terror-chief-al-qaeda-cyber/story?id=14224256> (noting that Al-Qaeda has specifically called for cyber attacks as they can be done remotely and individually); Duncan Gardham, *Terrorists are harnessing hi-tech communications, government warns*, TELEGRAPH (July 12, 2011), <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8633311/Terrorists-are-harnessing-hi-tech-communications-government-warns.html> (discussing Al-Qaeda’s guidance for individuals to act independently as they conduct “cyber jihad.”).

126. See, e.g., SINGER, *supra* note 84, at 264.

127. See QDR, *supra* note 4, at 37.

128. See, e.g., *Global Hacking Network Declares Internet War on Syria*, REUTERS (Nov. 30, 2012), <http://in.reuters.com/article/2012/11/30/syria-crisis-internet-anonymous-idINDEE8AT0C320121130> (“Global hacking network Anonymous said it will shut down Syrian government websites around the world in response to a countrywide Internet blackout believe aimed at silencing the opposition to President Bashar al-Assad.”).

129. See U.S. *Cyber Command: Organizing for Cyberspace Operations: Hearing Before the H. Comm. on Armed Services*, 111th Cong. 1 (2010) (statement of Rep. Skelton, Chairman, H. Comm. on Armed Services) (“[U.S.] information systems face thousands of attacks a day

becoming a regular occurrence as historically marginalized actors are drawn to the unprecedented opportunities—and limited risks—presented in the cyber domain.<sup>130</sup>

As cyber warfare becomes common, the international community cannot continue to rely on a static version of the existing law of armed conflict to resolve the “wicked” problems inherent in the “fifth domain.”<sup>131</sup> Only by looking beyond *lex lata*,<sup>132</sup> or how the existing law of armed conflict applies in cyber warfare,<sup>133</sup> and exploring *lex ferenda*,<sup>134</sup> or what the law in cyberspace should be, will States begin to develop solutions to the legal ambiguity that permeates cyber warfare and gain the clarity needed for operating in cyberspace. In modern warfare the “pace of change continues to accelerate,”<sup>135</sup> often straining the ability of the law of armed conflict to regulate contemporary conflicts. No emerging form of warfare creates more ambiguous legal questions than does cyber war, thus posing a great threat to the continued vitality of the law of armed conflict. Just as global militaries are adapting their doctrine, tactics and force structure to address the realities of cyberspace,<sup>136</sup> innovations in the law are necessary for effective regulation of this new domain. Addressing this threat is of paramount importance, as proactively keeping the law of armed conflict relevant maintains the delicate bal-

---

from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations.”).

130. See *id.* (statement of Rep. Skelton, Chairman, H. Comm. on Armed Services) (“[U.S] information systems face thousands of attacks from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations.”).

131. Along with land, sea, air and space, cyberspace is considered the fifth domain of warfare. See *War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25, available at <http://www.economist.com/node/16478792>. See also QDR, *supra* note 4, at 37 (“Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.”).

132. *Lex lata* is defined as “what the law is.” See J. Jeremy Marsh, *Lex Lata or Lex Ferenda? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MILITARY LAW REVIEW 116, 117 (2008).

133. TALLINN MANUAL, *supra* note 15, at 5. The *Manual* notes that its purpose is to explain the “law currently governing cyber conflict” and “does not set forth *lex ferenda*, best practices, or preferred policies.” *Id.*

134. *Lex ferenda* is defined as “what the law should be.” See Marsh, *supra* note 132, at 117.

135. QDR, *supra* note 4, at iii.

136. See, e.g., QDR, *supra* note 4, at 62 (“rising complexity in sea, air, space and cyberspace domains pose new security challenges that require innovative adjustments to our defense posture.”). See also Reeves & Barnsby, *supra* note 6, at 17 (discussing the adverse implications of a nation not recognizing new strands of warfare).

ance between military necessity and humanity, which ensures the primacy of the law remains unquestioned.