2014

New Hacktivists and the Old Concept of Levée En Masse

Christopher Waters
University of Windsor, Faculty of Law

Christopher Waters*

New Hacktivists and the Old Concept of *Levée en Masse*

The purpose of this article is to contribute to the continuing debate over the relevance of International Humanitarian Law (IHL) to cyberwar. It does so by taking what is often said to be a particularly archaic aspect of IHL, the French Revolutionary notion of levée en masse, *and asking whether the concept could have relevance in the cyber context. The article treats* levée en masse *as a litmus test for the law's relevance; if this IHL "relic" could have relevance in the cyber context, then the continued relevance of the larger body of rules should also be less doubtful.*

Cet article se veut une contribution au débat qui a cours sur la pertinence du droit humanitaire international (DHI) dans le contexte d'une cyber-guerre. Pour ce faire, l'auteur utilise ce qui est souvent qualifié d'aspect particulièrement archaïque du DHI, le concept français révolutionnaire de levée en masse, et demande si ce concept pourrait être pertinent dans le contexte du cyberâge. L'article traite la levée en masse *comme critère décisif de la pertinence de la loi; si ce vestige du DHI peut être pertinent dans le contexte du cyberâge, alors le maintien de la pertinence de l'ensemble des lois et des règlements devrait aussi être moins douteux.*

* Professor, Faculty of Law, University of Windsor. Earlier versions of this paper were presented at the Canadian Red Cross Conference on Cyberwarfare in Toronto in September 2013 and the Annual Conference of the Canadian Council on International Law in Ottawa in November 2013.

Introduction

It is common to suggest that war has changed significantly since International Humanitarian Law's (IHL) core instruments—the 1949 Geneva Conventions and their two Additional Protocols of 1977[1]—were drafted. For some, the ground has simply shifted too much for the rules to be meaningful, or at least for the rules to be implemented in their entirety.[2] Famously, a British defence minister went so far as to say in 2006 that unless we reconsidered the law "we risk continuing to fight a 21st Century conflict with 20th Century rules."[3] The shifting twenty-first-century terrain apparently involves the altered scope of the battlefield (including the urbanisation of warfare and the global war on terrorism) and the appearance of new actors on the battlefield (transnational armed groups and private military and security companies, among others). While a historian might point out that there is actually little new in any of these developments (and on the one hundredth anniversary of the start of World War I we might bear in mind that the trigger for the war was an act of

1. *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949, 75 UNTS 31; *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 12 August 1949, 75 UNTS 85; *Geneva Convention Relative to the Treatment of Prisoners of War*, 12 August 1949, 75 UNTS 135; *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, 75 UNTS 287. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 UNTS 3 [*Additional Protocol I*]; *Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, 8 June 1977, 1125 UNTS 609.

2. See, for example, Dan Belz, "Is International Humanitarian Law Lapsing into Irrelevance in the War on International Terror?" (2006) 7:97 Theor Inq L 6; Rosa E Brooks, "War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror" (2004) 153 U Pa L Rev 675 at 706; Gabor Rona, "International Law Under Fire: Interesting Times For International Humanitarian Law: Challenges from the 'War on Terror'" (2003) 27 Fletcher F World Aff 55. These concerns are not restricted to the English language literature. See, e.g., the Introduction to Abdelwahab Biad & Paul Tavernier eds, *Le droit international humanitaire face aux défis du XXIe siécle*, (Brussels: Bruylant, 2012).

3. Paul Reynolds, "The Rules of War: Too '20th Century?,'" *BBC News* (4 April 2006), online: <http://news.bbc.co.uk/2/hi/americas/4875694.stm>.

terrorism),[4] what cannot be denied is that new or emerging weapons, categorically different from what might have been anticipated in earlier decades, have appeared. Recent weapon technologies that may be game changers, posing an existential challenge to IHL, include nanotechnology, drones and automated weapons systems or "killer robots." Perhaps nowhere is the alleged unsuitability—even the quaintness—of IHL more apparent to sceptics than in the cyberwar context. As Wallace and Reeves, two West Point officers and law professors put it, "[a]pplying the law of armed conflict, as currently constructed, in this environment is 'highly problematic' as legal obligations are almost impossible to discern."[5]

The purpose of this paper is to demonstrate the continued relevance of IHL to cyberwar. It does so by taking what is often said to be a particularly archaic aspect of IHL, the French Revolutionary notion of a *levée en masse*, and asking whether the concept could have relevance in the cyber context. I treat *levée en masse* as a litmus test for the law's relevance; if this IHL relic could have relevance in the cyber context, then the continued relevance of the larger body of rules should also be less doubtful. Although drafted for broader purposes than a reply, this use of *levée en masse* as a test case may be considered the inverse of Wallace and Reeves's argument. They write:

> 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. 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.[6]

It would be facile to suggest that IHL treaties are perfect the way they are. It would be desirable to revise IHL by bringing the texts fully up to date with respect to the most modern means and methods of war. At the same time, it must be borne in mind that no sooner would the treaties be revised than the means and methods of warfare will have changed further. Whether it be e-commerce or reproductive technology, written law will generally

4. Namely the assassination of Archduke Franz Ferdinand, the heir to the Austro-Hungarian throne.

5. David Wallace & Shane R Reeves, "The Law of Armed Conflict's 'Wicked' Problem: Levée en Masse in Cyber Warfare" (2013) 89 Int L Stud 646 at 648.

6. *Ibid* at 649. Others have ignored *levée en masse* altogether, despite the concept's relevance to their arguments. For example, Susan W Brenner & Leo L Clarke "Civilians in Cyberwar: Conscripts" (2010) 43 Vanderbilt J Transnatl L 1011 at 1015 have compellingly demonstrated that "civilians are destined to play an active role in cyber hostilities" and discuss ways of conscripting civilians into cyber defence; however, they make no mention of *levée en masse*.

lag somewhere behind technical innovation. It would be foolish to say, however, that general contract law principles or family law principles do not apply to emerging technologies and cannot be purposively interpreted to meet new challenges.[7] My point here is that until the key IHL treaties are revised or a cyber-specific treaty regime put in place (and both of these scenarios seem unlikely in the near future), it is inaccurate and dangerous to suggest that IHL does not speak meaningfully to the questions which arise through the use of cyber or other emerging weaponry.

The interpretive evolution of law and the application of law to new facts, and indeed to changing conditions of life, are standard fare for lawyers. This is perhaps especially true for international lawyers. Article 31 of the Vienna Convention on the Law of Treaties provides that treaties should be interpreted in light of their "object and purpose"[8] and the International Court of Justice has not been shy about interpreting treaties in light of new developments.[9] Thus in holding that the word "commercial" included the transport of passengers under a nineteenth-century navigation treaty between Costa Rica and Nicaragua over the San Juan River, the Court said in 2009: "even assuming that the notion of 'commerce' does not have the same meaning today as it did in the mid-nineteenth century, it is the present meaning which must be accepted for purposes of applying the Treaty."[10] Furthermore, the Martens Clause in IHL treaties precludes static understandings of the law pertaining to international armed conflict. As first formulated in the Preamble to the 1899 Hague Convention (II) with respect to the laws and customs of war on land, it states:

> Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.[11]

---

7. On the application of the common law of contracts to e-commerce, see *ProCD v Matthew Zeidenberg and Silken Mountain Web Services Inc*, 86 F 3d 1447 (CA 7 Wis 1996).

8. *Vienna Convention on the Law of Treaties*, 23 May 1969, UNTS 1155, at 331 (entered into force 27 January 1980).

9. See generally, Campbell McLachlan, "The Evolution of Treaty Obligations in International Law" in Georg Nolte, ed, *Treaties and Subsequent Practice* (Oxford: Oxford University Press, 2013).

10. Case Concerning Navigational and Related Rights *(Costa Rica v Nicaragua)* Judgment, [2009] ICJ Rep 213 at para 70.

11. *Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land*, 29 July 1899, (entered into force 4 September 1900), online: ICRC <http://www.icrc.org/ihl.nsf/INTRO/150?OpenDocument>.

Although interpretations of the clause vary considerably (at its narrowest it means that customary law exists in parallel to treaty law and at its widest that humanitarian principles beyond hard law remain relevant),[12] the door is left open for normative evolution for the purposes of human protection. Finally, when constructing IHL treaties as a whole, it is important to note that the instruments specifically contemplate new means and methods of war. Notably, Additional Protocol I states that "it is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering" and requires that states ensure the development or use of new weapons complies with IHL.[13] Thus gone are the days when states could, albeit with limited plausibility, argue that aerial bombardment of civilians was unregulated since it was not specifically regulated.[14] With these principles in mind, we can turn in Part I to a brief exploration of the origins and nature of *levée en masse* and then, in Part II, probe its applicability in the cyber context.

I. Levée en masse

The French Revolutionary origins of the *levée en masse* are well established. Decisively turning a page on the traditional raising and commanding of armies by European princes, the Proclamation of the Revolution's National Convention of 16 August 1793 called for a mass levy of the French population: "From this moment until such time as its enemies shall have been driven from the soil of the Republic, all Frenchmen are in permanent requisition for the services of the armies."[15] As the revolutionary Bertrand Barère put it, "*Tout citoyen est soldat quand il s'agit de combattre la tyrannie*."[16] While the 1793 Proclamation was in one sense conscription, a governmental levy requiring all young men to fight and for other categories of citizen to attend to other duties, the *levée en masse* also represented a popular and "spontaneous" uprising against foreign invaders. The new force relied on patriotism, speeches

12. Rupert Ticehurst, "The Martens Clause and the Laws of Armed Conflict" (1997) 317 IRRC, online: ICRC <http://www.icrc.org/eng/resources/documents/misc/57jnhy.htm>. Furthermore, the International Law Commission, in commentary on its final draft articles on the law of treaties, observed that "[w]hen a treaty is open to two interpretations one of which does and the other does not enable the treaty to have appropriate effects, good faith and the object and purposes of the treaty demand that the former interpretation should be adopted." United Nations, *Yearbook of the International Law Commission 1966: Volume II*, A/CN.4/SER.A/1966/Add.1 (1967) at 219.

13. *Additional Protocol I*, *supra* note 1 at arts 35(2) and 36, respectively.

14. See R Nelson & C Waters, "The Allied Bombing of German Cities during the Second World War from a Canadian Perspective" (2012) 14 J Hist Intl L 87.

15. See generally WG Rabus, "A New Definition of the 'Levée en Masse," (1977) 24 NILR 232.

16. As cited in Rabus, *ibid* at 232.

and pamphleteering to raise men, and these fighters were not trained, disciplined or commanded in traditional fashion.

The concept of the citizen-soldier acting spontaneously in the face of a foreign invader was enshrined in various nineteenth-century legal instruments, including the 1863 Lieber Code, the 1874 Brussels Declaration and the Oxford Manual of 1880.[17] The 1899 and 1907 Hague Regulations codified the principle in treaty form, and the wording used by the Regulations has largely been carried over to the Third Geneva Convention of 1949. This latter Convention, the "Prisoners Convention," defines *levée en masse* for the purpose of determining who is a privileged belligerent entitled to prisoner of war status upon capture by the enemy. As explained by Henckaerts and Doswald-Beck, article 4(6) of the Convention states that the list of privileged belligerents includes

> [i]nhabitants of a non-occupied territory, 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. Aside from its provision in treaties, levée en masse also—uncontroversially it should be noted—has customary law status.[18]

Unlike other privileged combatants, participants in a *levée en masse*, driven by patriotism (or fear) to defend their country, do not need a regular command structure, uniform or distinctive insignia. The *levée* was conceptualized as being temporally limited to the time after an invasion and before occupation by the enemy or the incorporation of the citizen-soldiers into the army. In the view of many then, the *levée en masse* was a limited exception to IHL's usual categories of actors. The exceptional nature of this category is reflected in the Canadian 2001 Law of Armed Conflict (LOAC) Manual in its chapter on Combatant Status:

> As a general rule, civilians are considered non-combatants and cannot lawfully engage in hostilities. There is, however, an exception to this rule for inhabitants of a territory that has not been occupied by an enemy. Where they have not had time to form themselves into regular armed units, inhabitants of a non-occupied territory are lawful combatants if: a. on the approach of the enemy they spontaneously take up arms to resist the invading forces; b. they carry arms openly; and c. they respect the LOAC.

---

17. For a legal history of the concept, see Emily Crawford, "Regulating the Irregular: International Humanitarian Law and the Question of Civilian Participation in Armed Conflicts" (2011) 18:1 J Intl L & Pol'y 163.

18. Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules* (Cambridge: Cambridge University Press, 2005) at 384.

As Baxter describes the anomaly, "[t]he law of war has had to evolve an uneasy…compromise between the legitimate defence of regular belligerent forces and the demands of patriotism….The protected position afforded the members of the *levée en masse* is a monument to these sentiments…."[19]

There are clear World War II examples of *levée en masse*, including the resistance of the Cretan population in the face of a German invasion in 1941.[20] Contemporary examples are more limited.[21] In analysing the status of Bosnian Muslim forces around Srebrenica in 1992, where "very few individuals possessed a complete uniform" or other "fixed distinctive emblems recognisable at a distance," the International Criminal Tribunal for the former Yugoslavia (ICTY) Trial Chamber found that a *levée en masse* situation briefly existed.[22] Similarly, Georgian resistance had elements of *levée en masse* during the Russian invasion of Georgia proper in 2008, when young Georgian men drove towards the front lines and attempted to bolster regular forces.[23] The paucity of contemporary examples may be due in part to changing means of methods of conventional, non-cyber warfare. As Ipsen puts it,

> in modern-day armed conflicts the *levée en masse* has become less significant because, as a rule, the regular armed forces of an attacking party are armed to a degree that simply cannot be countered with the weapons available to a spontaneous resistance (such as hunting weapons).[24]

The more significant factor, however, may simply be the decline of international armed conflict vis-à-vis non-international armed conflict.

The lack of contemporary instances of *levée en masse* has led many to consider it an anachronism. For example, Solis suggests that "*levée en masse* may be a historical relic" and Draper posits that *levée en masse* is

19. Richard Baxter, "So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs" 28 (1951) BYIL 335.
20. Rabus, *supra* note 15.
21. Crawford, *supra* note 17.
22. *Prosecutor v Naser Orić*, IT-03-68-T, Judgment (30 June 2006) at para 135 (International Criminal Tribunal for the former Yugoslavia, Trial Chamber), online: ICTY <http://www.icty.org/x/cases/oric/tjug/en/ori-jud060630e.pdf>.
23. See Nicholas Kulish & Michael Schwirtz, "Sons Missing in Action, If Indeed They Found It," *The New York Times* (12 August 2008) A8, online: The New York Times <http://www.nytimes.com/2008/08/12/world/europe/12iht-12civilians.15190553.html?pagewanted=all&_r=0>.
24. Knut Ipsen, "Combatants and Non-Combatants" in Dieter Fleck, ed, *The Handbook of International Humanitarian Law*, 2nd ed (Oxford: Oxford University Press, 2008) at 94 .

"extremely rare and limited...."[25] However, despite the reports of *levée en masse*'s death, and the image of *levée en masse* as "an ignorant unruly crowd waving pitchforks about,"[26] there is no compelling reason to be rid of the category of fighter. Indeed, there is little reason to believe that the category will fall into desuetude in the long term; international armed conflict or invasions combined with spontaneous resistance by citizen-soldiers are unlikely to disappear. Furthermore, as the ICRC's customary law study points out, "While this exception may be considered of limited current application, it is still repeated in many military manuals, including very recent ones, and it therefore continues to be regarded as a valid possibility."[27] There are also conceptual reasons to keep it. As Emily Crawford writes, though without reference to the cyber context:

> Given the apparent difficulties in defining when a civilian is participating in armed conflict, the existence of a well-accepted set of rules that determine exactly when a civilian may legitimately participate in armed conflict is clearly advantageous. *Levée en masse* thus remains a useful, if infrequently used, categorisation. Its accepted position in custom and treaty law places *levée en masse* in the unique situation of being one of the very few international laws that legitimises civilian participation in international armed conflict. Given the long history of difficulties and resistance encountered whenever the laws of armed conflict relating to participants have been debated, the advantages of an existing, accepted law on civilian participation in armed conflict seems obvious.

Despite the arguments in favour of keeping *levée en masse*, it cannot be denied that the category arises rarely and strikes many as being anachronistic. At first glance then, if there is going to be any aspect of IHL which bears no applicability in most modern conflicts (aside perhaps from the protection of tobacco use by prisoners of war) and indeed shows the futility of applying IHL notions to cyberwarfare, it is *levée en masse*.

II. Levée en masse *in the cyber context*

In a ground-breaking 2006 article, Audrey Kurth Cronin called "cyber-mobilisation" the new *levée en masse*. She described how connectivity was being used to recruit and direct civilians in combat or terrorism, often using conventional weapons. But what of cyberwarfare itself rather than

25. Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge: Cambridge University Press, 2010) at 201. Ultimately Solis muses, "[p]erhaps future levées en masse...are not as improbable on today's battlefields as believed." GIAD Draper, "The Legal Classification of Belligerent Individuals" in Michael A Meyer & Hilaire McCoubrey, eds, *Reflections on Law and Armed Conflicts*, (The Hague: Kluwer Law International, 1998) at 202.
26. Rabus, *supra* note 15 at 232-233.
27. Henckaerts & Doswald-Beck, *supra* note 18 at 387.

cyber tools of command and control? Could hacktivists and others, using cyber weapons, constitute or be part of a *levée en masse*? In 2009 an expert consultative process on determining which, and how, rules of IHL could be applied in the cyberwarfare context was launched under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence. It resulted in the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[28] The Tallinn Manual is not unusual in the sense that there have been several reports in recent years which have sought to authoritatively clarify or provide operational guidance to states and commanders. These include the Copenhagen Process on detainees,[29] the *Manual on International Law Applicable to Air and Missile Warfare*,[30] and the ICRC's report on Direct Participation in Hostilities.[31] It is important to note that these reports have not purported to definitively establish or codify legal norms. The Tallinn Manual, which consists of 69 rules, makes a significant contribution to the discussion on how IHL applies in the cyberwar context. Rule 27 does, albeit tepidly and with serious qualification, provide for *levée en masse*. It states: "In an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status."[32] However, it appears from the commentary to the rule that the group of experts was divided on the *levée*'s continued relevance. The commentary suggests that while a *levée en masse* would be theoretically possible, it would nonetheless be improbable in the cyber context. Other observers, notably Wallace and Reeves, have reacted with incredulity to the notion that the *levée en masse* could have continued relevance.[33] There appear to be four main challenges to the continued currency of *levée en masse* in the cyber context. These challenges arise with respect to (1) the limited number of potential participants in a *levée en masse* (where is the *en masse*?), (2) whether a physical invasion needs to occur, (3) whether cyber defence could involve attacks behind the front lines and (4) how the requirement

28. Michael N Schmitt, ed, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013).

29. *Copenhagen Process on the Handling of Detainees in International Military Operations*, 19 October 2012, Ministry of Foreign Affairs of Denmark, online: <http://um.dk/en/~/media/UM/English-site/Documents/Politics-and-diplomacy/Copenhangen%20Process%20Principles%20and%20Guidelines.pdf >.

30. Harvard University HPCR, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, 15 May 2009, online: HPCR <http://www.ihlresearch.org/amw/manual/>.

31. Nils Melzer, *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (Geneva: ICRC, 2009).

32. Schmitt, *supra* note 28 at 102.

33. Wallace & Reeves, *supra* note 5.

that participants carry arms openly can be met. I consider these four challenges in turn.

First, as the Tallinn Manual itself says, "It is unclear whether *levée en masse* can be composed solely of a significant portion of the cyber-capable members of the population" as normally a *levée en masse* will involve a large segment of the population. It is true that not everyone has the means and expertise to participate in cyber warfare. However, not everyone engaged in a *levée en masse* need be capable of doing the same thing or in fact doing the same thing. In the original French *levée en masse*, the 1793 decree provided that "[t]he young men shall go to battle; the married men shall forge arms and transport provisions; the women shall make tents and clothes…."[34] In the cyber context, some participants may be identifying vulnerabilities in the enemy's target systems, others may be developing malware to exploit those vulnerabilities, and still others might participate in denial of service attacks or defences.[35] Furthermore, these sorts of attacks are integrally linked to online social networks, thus potentially opening up the cyber battlefield to millions of "netizens." Individuals using social media can play a role in cyberwar beyond merely propagandizing, mobilising and coordinating the population to resist. As James Carafano in his book *Wiki at War* puts it: "Almost any individual or group has the capacity to wreak some kind of online havoc, from stealing information and services to corrupting data, covertly monitoring or taking remote control of computers, and shutting down entire networks."[36] At any rate, there are perhaps fewer bright lines between cyber and conventional warfare than are sometimes thought; for example, the Stuxnet attack on Iran's nuclear program "featured many of the attributes of conventional military operations including intelligence operations and mid-operation fragmentary orders."[37] These activities may be centrally directed—as they certainly were in the Stuxnet attack—but may not be as well, at least not in any traditional sense of a command structure. But as *levée en masse* specifically excludes the need for a command structure this is not

34. "Decree Establishing the Levée en Masse, 23 August 1793" in David Ralston, *Soldiers and States: Civil-Military Relations in Modern Europe* (Boston: DC Heath and Company, 1966) at 66.

35. Paraphrasing Michael Schmitt, "Classification of Cyber Conflict" (2012) 17:2 JCSL at 256.

36. James Carafino, *Wiki at War* (College Station: Texas A & M University Press, 2012) at 111.

37. Sean Watts, "The Notion of Combatancy in Cyber Warfare" (paper delivered at the 4th International Conference on Cyber Conflict, Tallinn, 2012), (2012) NATO CCD COE Publications at 244, online: CCD COE <http://www.ccdcoe.org/publications/2012proceedings/4_2_Watts_TheNotionOfCombatancyInCyberWarfare.pdf>.

problematic.[38] Furthermore, the means and expertise to engage in cyber attack or defence are only increasing, leaving us with the curious possibility that *levée en masse* will become more relevant over time; that in fact cyber warfare will have breathed new life into an old concept. Citing examples from the Russian-Georgian and Arab-Israeli conflicts, among others, Heather Harrison Dinniss suggests, "[n]ot only are military networks a prime target for enemy forces, they come under increasing attack from civilians during times of war as well."[39] More recently, one can point to cyber attacks by Ukrainian and Russian "netizens" before and after the Russian occupation of Crimea in 2014 as evidence that cyberwarfare is not a phenomenon reserved to a few players.[40] It seems to me premature to declare that civilian engagement in cyberwar will not occur *en masse*.

The second challenge posed to the applicability of *levée en masse* is whether the category could apply in the case of a civilian population countering a cyber attack or whether a physical invasion by the enemy has to occur. The majority of experts for the Tallinn Manual thought that there had to be a physical invasion of national territory. The relevant provision of the Third Geneva Convention states that the *levée en masse* applies to "inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces." Unless we are going to take an "original intent of the framers" perspective reminiscent more of certain conservative strains in U.S. jurisprudence than international legal understandings of treaty interpretation, it is unclear to me why the enemy cannot "approach" in the cyber context.[41] It is a stretch to conceive of an invasion as purely occurring in the virtual world. Indeed, there must be violence at some point for IHL to apply at all—death to persons or damage to actual objects[42]—but once that happens there is, by its very nature, a kinetic invasion of sorts. Melzer has even argued that,

38. Ironically, as David Turns puts it: "Finally, 'hacktivists' generally—far from not having time to organize themselves—tend to be very well organized; indeed, it is the very concentration and intensity of their attacks that usually make them so effective." David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities," (2012) 17:2 J Confl & Sec L 279 at 293.

39. Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (New York: Cambridge University Press, 2012) at 172.

40. Nicole Perlroth, "Cyberattacks Rise as Ukraine Crisis Spills to Internet," *The New York Times* (4 March 2014), online: The New York Times <http://bits.blogs.nytimes.com/2014/03/04/cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/?_php=true&_type=blogs&_php=true&_type=blogs&hp&_r=1>.

41. For an account of the "original intent of the framers" perspective and a suggestion that the framers of the US Constitution themselves did not intend an ahistorical approach, see Powell H Jefferson, "The Original Understanding of Original Intent" (1985) 98:5 Harv L Rev 885.

42. Article 49 of *Additional Protocol 1*, *supra* note 1, states that attacks are "acts of violence against the adversary."

> [w]hile this category of persons has become ever less relevant in traditional warfare, it may well come to be of practical importance in cyberwarfare. Indeed, in cyber warfare territory is neither invaded nor occupied, which may significantly prolong the period during which a *levée en masse* can operate.[43]

The third major objection to the notion that *levée en masse* has continued relevance in the cyber context can be termed the "behind enemy lines" issue. Historically a *levée* was understood as involving a general uprising of the population to repel an invading force back across the national border; it did not comprise attacks deep into enemy territory. Could cyber operations by civilians, not against the actual invading forces but against military objectives well behind the lines, fit into this category? Again, on the language of the Third Geneva Convention, there is no need to exclude this possibility. But more broadly, under any interpretation of military necessity—a bedrock principle of IHL—there is no reason to limit cyber operations by defenders to countering the actual invading troops. Let us take an example from the 2008 Georgia-Russia war. Russia—presumably, but not conclusively, through state agents—quickly knocked out Georgia's cyber infrastructure.[44] According to the European Union's fact finding mission into the conflict:

> It looks quite apparent that significant cyber attacks were launched against Georgia in the course of the conflict. Most Georgian government [including the Ministry of Defence] and media sites were unavailable or defeated at some time during the first days of the conflict….Some experts believe that these attacks may have reduced Georgian decision-making capability.[45]

Presumably, these attacks were launched in Moscow, St. Petersburg or Sochi, and not by Russian troops and tank crews crossing the border. If territory is a non-factor in terms of the source of the cyber attacks then surely it must be in terms of the cyber defence required to repel it. Military necessity has limits naturally—as is often said, it must be balanced against the principles of humanity and distinction—but no such considerations arise in this case. If IHL is in any sense a practical regime, limiting cyber *levée en masse* defences to kinetic troops crossing a border would be an

43. Nils Melzer, "Cyberwarfare and International Law" (2011) UNIDIR at 34, online: UNIDIR <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.
44. Independent International Fact-Finding Mission on the Conflict in Georgia, *Report: Volume II* (September 2009) at 420, online: CEIIG < http://www.ceiig.ch/Report.html>.
45. *Ibid* at 217.

impractical result, creating a moral hazard where citizen defenders could not legally defend themselves.

The fourth challenge in applying levée en masse in the cyber context is the requirement to carry arms openly. Wallace and Reeves write:

> *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. This singular distinction requirement is not possible in a cyber war where the weapons are computers.[46]

The anonymous nature of civilian engagement with cyberwar is endemic and not a particular problem of *levée en masse*. Writing about cyberwarfare in the context of direct participation of hostilities, David Turns says:

> It is rather difficult to see precisely how these criteria could be applied in a cyber-conflict. Conceivably the taking up of arms could be loosely compared with the execution of CW commands against hostile systems, but how would they 'carry arms openly' in this context? Indeed, what would the 'arms' in question be—laptop computers, perhaps? If on the other hand the 'arms' are considered to be the software that executes the cyber attacks, how can they by nature ever be deemed to be carried 'openly'?[47]

These are legitimate questions. But, again, taking a purposive approach, we can ask what is at stake in the requirement to carry arms openly. Ultimately it is the perfidious use of weapons that poses difficulty, not camouflage or other ruses of war. Carrying one's weapons openly in the conventional context, even in the most literal-minded interpretation, does not of course mean that a citizen-soldier could not take cover behind an abandoned house or lie low in the bushes to avoid detection. As the ICRC Commentary to the Third Geneva Convention puts it with respect to resistance movements:

> [A]lthough the difference may seem slight, there must be no confusion between carrying arms "openly" and carrying them "visibly" or "ostensibly." Surprise is a factor in any war operation, whether or not involving regular troops. This provision is intended to guarantee the loyalty of the fighting, it is not an attempt to prescribe that a hand-grenade or a revolver must be carried at belt or shoulder rather than in a pocket or under a coat. The enemy must be able to recognize partisans

46. Wallace & Reeves, *supra* note 5 at 660. In fairness, Wallace and Reeves do not conclude that "anything goes" in cyberwarfare. Indeed they propose a creative solution, treating participants in a *levée en masse* more like irregular troops; although not needing to carry arms openly they would have other aspects of armed forces such as a command structure.

47. Turns, *supra* note 38 at 293.

> as combatants in the same way as members of regular armed forces, whatever their weapons. Thus, a civilian could not enter a military post on a false pretext and then open fire, having taken unfair advantage of his adversaries.[48]

Similarly, there is no principled reason why a citizen-hacktivist cannot seek to avoid detection when attacking lawful targets. And, as a practical matter, if detection occurs, he or she is of course targetable. What the hacktivist cannot do is use a hospital or school computer or network for launching cyber attacks. As Melzer has suggested, "a possible solution would be to consider this requirement [to carry arms openly] as fulfilled when cyber operations are not conducted by feigning protected, non-combatant status within the meaning of the prohibition of perfidy."[49] Sean Watts also adopts a functional approach to distinction generally, arguing that

> [f]ar more than the outward appearance of individuals conducting CNA [Computer Network Attacks], distinction in CNA demands attention to the actual conduct of the attack—the target chosen, the pathways of entry, and the means used to achieve destruction or other harmful effects.[50]

Admittedly, one of the problems of taking this functional approach is that it may conflate the requirement to carry arms openly with the other criteria of the definition of *levée en masse*, namely the obligation to respect the laws of war. However, it does represent a viable and practical approach to interpreting Article 4 of Geneva Convention III in light of technological developments.

This paper's argument that a hacktivist may be a lawful combatant in the face of a cyber or kinetic invasion underscores the importance of the obligation to respect the laws of war. Dinstein suggests that this latter criterion

> is the key to understanding the philosophy underlying the distinction between lawful and unlawful combatants. Unless a combatant is willing himself to respect LOIAC [Law of International Armed Conflict], he is estopped from relying on that body of law when desirous of enjoying its benefits.[51]

---

48. Jean de Preux, *Commentary on the Geneva Conventions of 12 August 1949,* Vol III (Geneva: ICRC, 1960) at 61.

49. Melzer, *supra* note 43 at 34.

50. Watts, *supra* note 37 at 246.

51. Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 2nd ed (Cambridge: Cambridge University Press, 2004) at 39. Rabus, *supra* note 15 at 240, goes further, arguing that the treaty provisions on *levée en masse* should be amended to drop the requirement to carry arms openly and to maintain only the obligation to respect the laws of war.

If it is the case that the gravamen of the *levée en masse* is that when the population is defending itself against assailants it must respect the laws of war, then, to paraphrase Rabus,[52] what is needed is a serious effort to disseminate IHL norms to cyber aware and cyber capable populations. This need has been identified by the ICRC, among others, although states (despite their dissemination obligations with respect to civilian populations) have done little in this regard.[53] Whether as participants in a *levée en masse* or in some sort of other lawful combatancy, the ability of hacktivist-combatants to understand and apply the basic principles of IHL will be crucial to their status and more importantly, to the protection of the civilian population and other potential victims of warfare. This leads to a final point, or at least a final question. Leaving aside moral imperatives to comply with the substance of the law, the flip side of the arguments for inclusion of hacktivists within a category of lawful combatants is as follows: if they can't be lawful combatants when striving to act lawfully, then why obey the laws of armed conflict at all?

Conclusion

It is not the intent of this article to suggest that *levée en masse* is an ideal fit with cyberwarfare. The notion of hacktivists acting spontaneously and *en masse* may indeed be a stretch, although, as suggested above, paradoxically cyberwarfare may make the concept more relevant than ever. But I have attempted to make the argument here that even in the face of one of IHL's so-called obsolete categories, a category only tepidly and reluctantly recognised by the drafters of the Tallinn Manual and derided by others as being an absurdity in modern warfare, the key IHL treaties remain relevant and adaptable. There may be a better way to deal with cyberwarfare—through revised Geneva Conventions, through a dedicated cyberwarfare treaty or through the creation of an international cyber security organisation among other options. Until then it should be made

52. Rabus, *supra* note 15 at 237.

53. While more discretion is given to states with respect to dissemination among the civilian population, as opposed to military personnel, in the Geneva Conventions Article 83 of *Additional Protocol I*, *supra* note 1, provides that:"The High Contracting Parties undertake, in time of peace as in time of armed conflict, to disseminate the Conventions and this Protocol as widely as possible in their respective countries and, in particular, to include the study thereof in their programmes of military instruction and to encourage the study thereof by the civilian population, so that those instruments may become known to the armed forces and to the civilian population." Though not directed at the norms of cyberwarfare per se, the ICRC's dissemination efforts with respect to video gaming may be of particular importance in reaching young cybercitizens; see ICRC, "Video Games and the Laws of War," online: ICRC <http://www.icrc.org/eng/resources/documents/film/2013/09-28-ihl-video-games.htm>.

clear that there is a body of law regulating cyber means and methods of war.[54]

54. A point made by Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians" (2012) 94:886 IRRC 533 at 540; Michael Gervais, "Cyber Attacks and the Laws of War" (2012) 30 BJIL 525.