2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

The Notion of Combatancy in Cyber Warfare*

Sean Watts
Creighton University Law School
Omaha, Nebraska, U.S.A.
United States Military Academy at West Point
West Point, U.S.A.

Abstract: The class of combatant constitutes one of the most important instrumentalities of the law of war. Combatant status resolves critical and enduring legal questions such as immunity from prosecution for warlike acts, susceptibility to intentional targeting, and, in part, treatment upon capture. Since the late nineteenth century, codifications of the international law of war have included criteria for combatant status keyed to ensuring desirable battlefield conduct and, to the extent possible, humanity in war. This paper revisits the author's prior work on the topic of combatancy in cyber warfare. Building on recent public revelations concerning state capacity for offensive cyber attacks, as well as new developments in computer network attack, this paper highlights logical and normative shortcomings in current understandings of combatant status in cyberspace. In place of rote reliance on existing criteria intended for the kinetic battlefield, this paper proposes reliance on State affiliation as the sole criterion for evaluating combatant status in cyber warfare between States. An admitted interpretive gloss on current criteria, the proposed framework offers a workable and realistic reconciliation of humanitarian goals and emerging State practice in cyber warfare.

Keywords: *International Humanitarian Law, Law of Armed Conflict, Law of War, cyber attack, cyber warfare, combatant status*

1. INTRODUCTION

The laws of war occasionally paint an idealized portrait of armed conflict. An impression of war formed exclusively from the international legal instruments that regulate the conduct of hostilities would render an image perhaps foreign to present day combatants. In lieu of surprise attacks, one would find punctilious declarations of hostilities in the form of diplomatic notes or ultimatums.[1] States would investigate detention conditions and communicate their humanitarian

* This paper updates concepts and ideas developed previously and in greater depth in *Combatant Status and Computer Network Attack*, 50 Virginia Journal of International Law 392 (2009)[hereinafter Watts].

1 Convention Relative to the Opening of Hostilities, art. 1, Oct. 18, 1907, 36 Stat. 2259, 1 Bevans 619 [hereinafter 1907 Hague Convention III](requiring that contracting Powers not commence hostilities "without previous and explicit warning).

concerns to one another through mutually acceptable third State parties.[2] Combatants would make themselves physically separate and visually distinguishable from civilians through the wear and display of distinctive uniforms and insignia.[3] Civilian populations would be warned in advance of impending attacks and provided an opportunity to evacuate to safe areas.[4] Safety zones, immune from attack would be created in the midst of the battlefield to provide shelter to children and the elderly.[5] And belligerents would facilitate the transport of wounded by air through agreed flight plans for medical aircraft, even through enemy territory.[6]

The reality of modern warfare is, of course, quite different. States rarely resort to declarations of war any longer. The Geneva Conventions' Protecting Power scheme almost never operates through third party States. The modern battlefield sees fighters intermingled with and often indistinct from their civilian counterparts. The opportunity to warn civilians of impending bombardments or attacks, without dooming such operations to failure, rarely presents itself. Civilians are all-too-often caught up in or the object of military attacks. And, as yet, agreements between belligerents permitting enemy medical aircraft to fly over friendly-controlled territory have not become standard operating procedure.

Yet it is too much to say that the law of war is entirely irrelevant or ineffectual. It is still probably correct to say that most States regard the law of war as more than merely epiphenomenal. In fact, States' militaries and government agencies have largely internalized and rendered operational the great majority of the present laws of war. For example, the proliferation of serious military legal manuals provides doctrinal evidence that States regard the law of war as relevant and meaningfully binding.[7] In an era when many armed forces face personnel cuts, reliance on sizable corps of military and civilian lawyers to review and advise on planning and operations reflects States' real commitment to the notion of legal restraint in war. And prosecutions at international criminal tribunals reflect both States' willingness to dedicate significant resources to the law as well as their commitment to enforce at least the principles, if not always the exact

2 Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 8, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter 1949 Geneva Convention I]; Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 8, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter 1949 Geneva Convention II]; Convention Relative to the Treatment of Prisoners of War art.8, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter 1949 Geneva Convention III]; Convention Relative to the Protection of Civilian Persons in Time of War art. 9, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter 1949 Geneva Convention IV](concerning the appointment of Protecting Powers by parties to an international armed conflict for purposes of implementing the 1949 Geneva Conventions).

3 1949 Geneva Convention III, *supra* note 2, art 4A(2)(b); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 44(7), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I](incentivizing display distinctive insignia and wear of uniforms by combatants through conferral of prisoner-of-war status).

4 Protocol I, *supra* note 3, art. 57(2)(c); Convention Respecting the Laws and Customs of War on Land, Annex to the Conventions, art. 26 Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter 1907 Hague IV Regulations].

5 1949 Geneva Convention IV, *supra* note 2, art. 14.

6 Protocol I, *supra* note 3, arts 26 & 29.

7 *See e.g.* United States Department of the Navy, The Commander's Handbook on the Law of Naval Operations, NWP1-14M, (July 2007); United Kingdom Ministry of Defence, The Manual of the Law of Armed Conflict (2004); Canadian Office of the Judge Advocate General, Law of Armed Conflict at the Operational and Tactical Levels (Aug. 13, 2001); Federal Republic of Germany, Federal Ministry of Defence, (Aug. 1992). A study of customary international laws of war by the International Committee of the Red Cross draws on a far broader sampling of States' law-of-war manuals. 2 Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law (2005).

letter, of existing international law regulating the conduct of hostilities.[8]

Owing to disparity between the letter of the law of war and its practical implementation, much of States' adherence to the law of war relies on secondary rules.[9] So often drafted long before the evolutions and revolutions in the wars they regulate, law-of-war treaties frequently require adaptive understandings, interpretive canons, or operational implementation – so-called secondary rules – to remain relevant. In addition to supporting claims of general legal efficacy, military manuals, military lawyers, and international criminal trials each contribute to States' efforts to adapt existing law to the evolving realities of armed conflict. Law of war manuals contextualize obligations, providing interpretation and examples of implementation. Military lawyers operationalize legal principles and rules through advice during planning and execution of orders, adapting law to battlefield conditions and evolving threats. And tribunals, domestic and international, perform a similar function, interpreting and applying law-of-war terms, often according to their perceived object and purpose. In short, although faced with idealized expressions and often dated assumptions, States continue to honor the law of war aided by a variety of interpretive measures. Interpretation vindicates the law by ensuring its relevance and vitality, operationalizing humanitarian ideals to the extent possible while assuring military effectiveness and realism.

This paper seeks briefly to illustrate and defend such an interpretation in the context of an emerging and revolutionary form of warfare – cyber war. This paper will briefly address the important question of combatancy or combatant status in cyber warfare. In particular, the question of who may directly participate in cyber hostilities will be addressed. If States have developed a class of cyber warriors, must they be drawn from or incorporated into regular armed forces? Or may a State sanction and employ civilian actors to conduct cyber attacks and other warlike operations in cyberspace?

Like many law-of-war provisions, the criteria for combatant status are derived from long-standing traditions. Chosen both to reflect and to reinforce classic attributes of legitimate belligerents, the combatant criteria perform gate-keeping functions for both prisoner of war status, and immunity from prosecution for lawful warlike acts as well as the critical question of exposure to intentional targeting. While well-suited to the battlefields of centuries past, I argue that the traditional combatant criteria are applied over-broadly to participants in emerging forms of remote warfare such as computer network warfare. Increasingly these rules misapprehend how and, more importantly, by whom modern war such as cyber warfare will likely be fought.

This paper proposes an alternate test for combatant status in cyber warfare focused on State affiliation. Long an important, yet overlooked criterion for combatant status, State affiliation enjoys solid textual support in the extant law and supports the fundamental principles of distinction and discipline through State responsibility. But perhaps most importantly, State affiliation as a criterion for lawful combatancy in cyber warfare is minimally disruptive to emerging State practice thus guaranteeing relevance and alignment of the law with the realities

8 *See* Prosecutor v. Gotovina et al., IT-06-90-T, 15 Apr. 2011 (sentencing two senior Croatian military officers to 24 years and 18 years confinement for indiscriminate artillery shelling and a joint criminal enterprise to persecute and deport ethnic Serbians).

9 The English legal philosopher H.L.A. Hart identified secondary rules as rules that give effect to primary rules that directly regulate conduct. Rules of adjudication, interpretation, and that prescribe the operation of primary rules constitute secondary rules. H.L.A. Hart, The Concept of Law, 77-79, 88-93 (1961).

of the cyber battlefield. State affiliation as a stand-alone sole criterion is admittedly a gloss on the present law of combatant status, perhaps at this point more in the nature of *lex ferenda*. However it is an interpretation that overcomes the existing law's static and dated character, augmenting its legitimacy by reconciling what States say with what States actually do and will do in cyber warfare.[10]

2. THE INTERNATIONAL LAW OF COMBATANCY

In contrast to its public international law cohort, international human rights law, the law of war has long relied on classifications to allocate protections, duties, and responsibilities.[11] Where the protections of human rights law apply merely by virtue of personhood, law-of-war protections have generally been contingent upon persons' satisfaction of particular criteria, such as nationality, membership in an organization, or a prescribed course of conduct. Presently, the most important law-of-war classifications with respect to persons are the civilian and combatant classes. This section briefly outlines the traditions, legal framework, and consequences of the law-of-war status of combatant.

The earliest attempts to draft multilateral law-of-war treaties recognized the status of combatant, beginning with the 1874 Brussels Declaration.[12] Designed to capture the customs and usages of militaries that alleviated unnecessary suffering in war, the Declaration applied the "laws, rights, and duties of war . . . not only to armies, but also to militia and volunteer corps fulfilling the following conditions:

1. That they be commanded by a person responsible for his subordinates;
2. That they have a fixed distinctive emblem recognizable at a distance;
3. That they carry arms openly;
4. That they conduct their operations in accordance with the laws and customs of war."[13]

The Declaration's description of the combatant class was noteworthy in several respects. First, the Declaration's definition was an expansive conception of the combatant class. The definition included not merely States' regular armed forces but also irregular or mustered volunteers. It was at once progressive and conventional. The definition would give international recognition and legal status to emergent fighting forces, yet by qualifying their combatant status on satisfaction of the four enumerated criteria, the Declaration incentivized conformity with the traditional behaviors, appearances, and customs of States' regular armed forces. Since the Declaration was drafted, States have continued to debate the merits of legal recognition of unconventional fighting organizations. Yet as recently as 2002, States have identified the four criteria as essential attributes of organized armed forces, including a controversial U.S. legal opinion requiring that even regular armed forces fulfill the four 1874 criteria to legitimately

10 *Id*.

11 Although dispute exists as to the geographic applicability of many human rights norms and treaties, once activated human rights obligations are generally accepted as universally applicable to all persons, regardless of citizenship, national origin, or political alliance.

12 Project of an International Declaration Concerning the Laws and Customs of War, Aug. 27, 1874, 4 Martens Nouveau Recueil (ser. 2) 219 [hereinafter 1874 Brussels Declaration]. Despite its seemingly fundamental protections, the Declaration appears to have gone too far for most of its signatories as it never entered force. *See* The Laws of Armed Conflicts 21 (Dietrich Schindler & Jiri Toman, eds., 2004).

13 1874 Brussels Declaration, *supra* note 9, art. 9.

claim combatant status.[14]

The Declaration's description of the combatant class is also noteworthy for its longevity. Although the Declaration never entered into force itself, succeeding multilateral law-of-war treaties liberally incorporated its definition. The 1899 Hague Convention II,[15] the 1907 Hague Convention IV Annexed Regulations,[16] the 1929 Geneva Prisoners of War Convention,[17] and the 1949 Third Geneva Convention[18] all reproduce or incorporate the 1874 criteria by reference in their descriptions of combatants. With the important exception of a clearer reference to the requirement of State affiliation in the 1949 Third Geneva Convention, the 1874 criteria operated nearly unchanged for over 100 years.[19] Not until 1977, with Additional Protocol I to the Geneva Conventions, did the international law of war tinker with the 1874 Declaration's formula for combatant status. Yet even Additional Protocol I remained grounded in the 1874 criteria to a significant extent.

Polemical accounts criticize Additional Protocol I for rendering meaningless the class of combatant.[20] Such critiques focus on the Protocol's abandonment of the traditional combatant criteria. It is true that the Protocol's modification of the 1874 criteria drew significant dissent, including a number of reservations by States Parties,[21] as well as refusals to ratify by States attending the diplomatic conference.[22] Closer examination, however, reveals the persistent, though marginally reduced, influence of the 1874 criteria.

Additional Protocol I defines combatants as "[m]embers of the armed forces of a Party to a conflict [...]"[23] Elaborating on the term "armed forces" the Protocol adds,

> "The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict."[24]

14 Memorandum from Jay S. Bybee, Assistant Att'y Gen., Office of Legal Counsel, Dep't of Justice, to Alberto Gonzales, Counsel to the President, and William J. Haynes II, Gen. Counsel of the DOD, *Application of Treaties and Laws to al Qaeda and Taliban Detainees* 10 (Jan. 22, 2002) in The Torture Papers (Karen J. Greenberg & Joshua L. Dratel eds., 2005).

15 Convention with Respect to the Laws and Customs of War on Land, art. 1, July 29, 1899, 32 Stat. 1803, 26 Martens Nouveau Recueil (ser. 2) 949.

16 1907 Hague IV Regulations, *supra* note 4, art. 1.

17 Convention Relative to the Treatment of Prisoners of War, art. 1(1), July 27, 1929, 47 Stat. 2021, 118 L.N.T.S. 343.

18 1949 Geneva Convention III, *supra* note 2, art. 4A(2).

19 *Id*. (prefacing the four 1874 criteria with, "Members of militias and members of other volunteer corps, including those of organized resistance movements *belonging to a Party to the conflict* [...].")(emphasis added).

20 Douglas J. Feith, *Law in the Service of Terror*, The National Interest (Fall 1985).

21 *See* United Kingdom Reservations to Additional Protocol I to the Geneva Conventions (July 2, 2002), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument.

22 *See e.g*. Letter of Transmittal and Letter of Submittal Relating to Protocol II Additional to the Geneva Conventions of 12 August 1949 (Jan. 29, 1987), *reprinted in* U.S. Dep't of the Navy, Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, 306 (A.R. Thomas & James C. Duncan eds., 1999).

23 1977 Additional Protocol I, *supra* note 3, art. 43(2).

24 *Id*. art. 43(1).

The influence of the 1874 criteria is obvious. Even under the Additional Protocol's relaxed rules for combatancy fighting organizations must still appoint and take direction from a superior commander and must conform their conduct of hostilities generally to the law of war. In fact, Additional Protocol I only departs from two of the four 1874 criteria and does so only in a limited sense. In fact, article 44 requires that combatants "distinguish themselves from the civilian population" and "carr[y] arms openly." Facially, the latter requirement with respect to carrying arms makes no change to the traditional rule. The former requirement with respect to distinction, although abandoning the 1874 phraseology, also performs substantially the same function as its forebear. Rather than dispense with uniforms and military insignia entirely, the Protocol's phrasing merely seems to admit alternate visual indicia of fighting organizations' hostile function, such as clothing or armbands.[25]

The only notable Additional Protocol I alteration to the 1874 criteria concerns a limited exception for guerilla fighters and insurgent groups in enemy-occupied territory. Article 44 relaxes the distinction and arms criteria when "owing to the nature [...] [of] hostilities," observance would be impracticable.[26] The exception is not available during attacks or when visible to enemy forces while preparing for or deploying to attack. Concerned with the negative implications for civilian populations, the majority of delegations to the Additional Protocol's diplomatic conference understood the exception to be limited to non-combat related movements in occupied territory.[27] In the vast majority of circumstances related to combat, the four 1874 criteria operate under Additional Protocol I has they had for over a century. Thus, in the majority of circumstances even Additional Protocol I preserves the four 1874 criteria as the essential prerequisites to combatant status.

The 1874 Declaration and its criteria are also remarkable for their attention to the realities and demands of late nineteenth and early twentieth century warfare. Each criterion performed an important function in ensuring warfare between States was distinguishable from uncontrolled violence. The first criterion, the responsible command requirement, ensured that lawful participation in warfare was limited to organized groups operating on behalf of States. The responsible command function excluded individual opportunists, criminals, and brigands from combatant status. Additionally, the command criterion aided accountability and adherence to law, ensuring superiors presumably better steeped in the traditions and customs of lawful combat supervised their combatants' actions. One found on the battlefield, and one often still finds today, an environment ripe for criminal exploitation. Suspended civil capacity, vulnerable and displaced populations, damaged or abandoned property, and general chaos present convenient conditions for looting, rape, and other criminal activity. Additionally, in war, individual armed belligerents often wield power out of proportion to their authority. Command and the attendant systems of internal discipline emblematic of armed forces stood as essential deterrents to battlefield bedlam. Military command structures, with their strict hierarchies and rigorous lines of authority, operated effectively despite physical and geographic separation between the leader and led. Military command ensured that combatants limited their conduct to actions that were militarily necessary.

The second and third of the 1874 criteria, that combatants wear distinctive emblems and carry

25 *See* Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 527-28 (Yves Sandoz et al. eds., 1987)[hereinafter Additional Protocol Commentary].
26 *Id*. art. 44(3).
27 *See* Additional Protocol Commentary, *supra* note 20, at 530-32.

arms openly, also performed an important battlefield function related to humanity and civility. Uniforms and the open display of military arms greatly facilitated opposing forces' efforts to distinguish enemy combatants from civilians. With engagements limited to visual range, displays of distinctly military uniforms and weapons were a particularly effective means of limiting the effects of hostilities to combatants on the late nineteenth century battlefield. Nor did the twentieth century's widespread use of beyond-visual-range or over-the-horizon weapons render the uniform and arms criteria useless. Line-of-sight engagements remained prevalent features of twentieth century kinetic armed conflict. Moreover, forward observers or other combatants directing and adjusting the fire of indirect and over-the-horizon weapon systems could still rely on uniforms and the open display of weapons to distinguish lawful targets from protected civilians.

Last, the requirement that combatants' organizations conform their conduct to the laws and customs of war performed an important reinforcing function. A form of reciprocity, the fourth 1874 criterion excluded from the combatant class groups of fighters unwilling to adhere to traditional and recognized limits on the conduct of hostilities. Members of groups regularly resorting to perfidy, treachery, indiscriminate attack, use of prohibited weapons, or maltreatment of victims of war could not claim the law's protections accorded to combatants upon capture. Requiring that combatant organizations conduct their operations in accordance with the law of war also incentivized individual instruction in the law to guarantee continued combatant status and its attendant protections and privileges. Physically separated from and often out of communication with legal advisors and senior leaders, nineteenth and twentieth century combatants could be distinguished from their unlawful belligerent counterparts for the internal familiarity with and general observance of the rudiments of lawful battlefield conduct.

No explanation of combatancy under the law of war would be complete without discussion of its functions. Like all forms of status under the law of war, combatant status is a legal instrumentality – a means of prescribing and allocating legal obligations and protections. In short, three consequences flow from assignment of combatant status – only one of which is exclusive to that class.

The most important and the only exclusive consequence of combatant status is immunity from prosecution for lawful warlike acts. It is widely accepted that combatants may not be brought to criminal trial for acts of destruction or killings they commit in war.[28] Although combatant immunity (also known as the combatant's privilege) is well-established in the customs of war, the principle appeared relatively late in the codified laws of war. Additional Protocol I of 1977 appears to be the first multilateral codification of combatant immunity, providing, "Members of the armed forces [...] have a right to participate directly in hostilities."[29] While debate exists whether direct participation in hostilities by persons not qualifying as combatants constitutes an individual criminal offense under international law, it is quite clear that neither international nor domestic criminal tribunals may prosecute the otherwise lawful warlike acts

28 Anicee van Engeland, Civilian or Combatant? A Challenge for the 21st Century, 45 (2011); Knut Ipsen, *Combatants and Non-Combatants, in* The Handbook of Humanitarian Law in Armed Conflicts 81 (Dieter Fleck ed., 1995).

29 1977 Additional Protocol I, *supra* note 3, art. 43(2).

of combatants.[30] Acts of combatants that violate discreet law-of-war rules are punishable, such as perfidy, indiscriminate attack, use of unlawful weapons or means of war, or maltreatment of protected persons. However, the mere fact of combatants' direct participation in hostilities itself is privileged and perhaps the most significant by-product of combatant status.

A second consequence of combatant status is conferral of prisoner of war status upon capture. The concept of prisoner of war is ancient and has included progressively comprehensive protections as the law-of-war has developed.[31] In general, captors may only impose restraints on the liberty of prisoners of war necessary to prevent their return to the battlefield. Properly carried out, prisoner of war detention has more in common with camp or internment settings than with criminal incarceration. Prisoners of war are guaranteed payment, protection from abuse, recreational opportunities, limits on forced labor, significant procedural protections from discipline and punishment, communication with family members, and regular medical treatment.[32] Upon termination of hostilities, detaining powers must repatriate prisoners of war to their countries of origin. Unlike combatant immunity, prisoner of war status is not exclusive to combatants. At least two classes of civilians are also entitled to prisoner of war status upon capture: contractors, correspondents, and laborers accompanying the armed forces; and crews of merchant marine ships and civil aircraft used by belligerents.[33]

The final significant consequence of combatant status is exposure to status-based targeting by enemy forces. Combatants are lawful targets for their enemies' operations at all times until their surrender, capture, or incapacitation by wounds.[34] It is their status as combatants, their formal affiliation with and conduct of hostilities on behalf of an enemy State in international armed conflict, rather than their conduct that makes combatants lawful targets. Whether a combatant is in uniform or not, on duty or not, conducting an attack, or sleeping, she is a lawful target for enemy forces. Classically, status-based susceptibility to targeting has been a condition unique to the combatant class.[35] While civilians are subject to lawful targeting while taking direct part in hostilities, they are only lawful targets "for such time as" or while they actually commit hostile acts directly producing harmful effects to an enemy.[36] In this respect hostile civilians can be said to be targetable only on the basis of their conduct rather than any status. However, recently the exclusivity of combatants' status-based exposure to targeting been challenged widely.[37]

Thus, combatant status constitutes a central and remarkably static feature of the regulation of hostilities. From the time when war featured massed formations of distinctly-clad soldiers

30 *See* Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerillas, and Saboteurs*, 28 Brit. Y.B. Int'l L. 323 (1951); Knut Dörmann, *The Legal Situation of "Unlawful/Unprivileged Combatants*," 85 Int'l Rev. Red Cross 45 (2003). For discussion of whether direct participation in hostilities by persons not qualifying for combatant status constitutes a crime under the international law of war see Mark David 'Max' Maxwell & Sean Watts, *'Unlawful Enemy Combatant': Legal Status, Theory of Culpability, or Neither*, 5 Journal of International Criminal Justice 19 (2007).

31 For an exceptionally thorough treatment of prisoner of war status, see 59 International Law Studies: Prisoners of War in International Conflict (Howard S. Levie, ed., 1979).

32 See 1949 Geneva Convention III, *supra* note 2, Part III.

33 1949 Geneva Convention III, *supra* note 2, art. 4(A)(4) & (5).

34 *See* Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, 34 (2d ed., 2010).

35 A recent study sponsored by the International Committee of the Red Cross with growing international support appears to extend status-based targeting to members of so-called organized armed groups. Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, 31-35 (2009).

36 1977 Additional Protocol I, *supra* note 3, art. 51(3).

37 See Interpretive Guidance, *supra* note 35.

facing off with short-range rifles to the age of transcontinental missiles and remotely-piloted attack drones, relatively little with respect to the legal qualifications for or consequences of combatancy has changed. The following section inquires whether the static nature of combatancy is appropriate in light what is known and expected to develop in the emerging forms of conflict such as cyber warfare.

3. COMBATANCY IN CYBER WARFARE

In a prior article addressing the topic of combatant status and computer network attack, I used incidents in Estonia in 2007 and in Georgia in 2008 to illustrate the nature and effects of hostile computer network operations.[38] For authors addressing the legal aspects of cyber warfare at that time, the Estonian and Georgian directed denial of service incidents offered the most prominent, publicly available examples of international computer network incidents intended to harm States. Yet each incident offered minimal assistance in illustrating the operation of law-of-war principles in the cyber context. As most experts would agree, neither incident on its own constituted an "attack" for purposes of the law of war. Viewed alone, each likely amounted to a mere disruption of communications or inconvenience. At best, the Estonian and Georgian incidents illustrated the likelihood that States could impose significant disruptions through cyber means and would likely dedicate significant resources in the future to developing and countering cyber capacity to carry out cyber operations that might truly amount to attacks in the legal sense.

Since the Estonian and Georgian incidents, two developments have better framed the realities of computer network attack (CNA). First, one need no longer speculate or read between the lines of budget requests, as I did earlier, to determine whether States possess offensive cyber capacity. States have made clear that cyberspace is an important military domain.[39] Some States have even publicly acknowledged their capacity for offensive cyber operations amounting to attack.[40] A recent United States Defense Authorization Act curiously includes the following, "Congress confirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace [...]."[41] And in a 2011, statutorily required report to the United States Congress, the Department of Defense revealed publicly, "[T]he Department has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests. If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict."[42] Thus, it is

38 See Watts, *supra* note *, at 397-407.

39 *See e.g.* United States Department of Defense, *Strategy for Operating in Cyberspace*, 5 (2011) (resolving to treat cyberspace as operational domain).

40 *See* Uzi Mahnaimi, *Israeli Military Plots to Cripple Iran in Cyberspace*, London Sunday Times (Aug. 7, 2011) (describing an Israeli military cyber command reporting directly to the Prime Minister)[herinafter Mahnaimi].

41 2012 National Defense Authorization Act, sec. 954.

42 United States Department of Defense, *Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, 5 (Nov. 2011) [hereinafter *Cyberspace Policy Report*].

clear that States have developed internal capacity, including cadres of cyber warriors, dedicated to conducting network warfare.[43]

A second development confirming the nature and extent of hostile cyber capacity is the 2010 Stuxnet worm attack on Iran. Discovered publicly in July of 2010, Stuxnet was a complex, malicious code believed to have been designed and introduced to sabotage industrial control systems in the Iranian nuclear program.[44] Combining an array of at least nine distinct variants of malware, including four invaluable zero day exploits, Stuxnet first infected Windows-based computers then spread to others in search of its target industrial control systems.[45] Although initially introduced to relatively few systems, Stuxnet later self-replicated to affect many more target systems.[46] It also appears the creators of Stuxnet updated and improved the worm as the attack unfolded. Earlier infected systems even requested and received updated versions of Stuxnet.[47] Once embedded in its final target system, Stuxnet modified and provided faulty performance feedback to control systems causing those systems to issue destructive operating commands to the machines they controlled.[48] It is estimated that Stuxnet caused sufficient physical damage to Iranian nuclear industrial apparatuses to set the program back one to two years.[49] To many, the unprecedented sophistication of the operation suggested that only State actors could have launched the attack.[50]

More so than previously revealed cyber operations, Stuxnet illustrates the potential of cyber operations to rise the level of attack under the law of war. If the hallmark of attack under the law of war is physically destructive effects, Stuxnet clearly qualifies. Stuxnet makes clear that crippling and physically destructive attacks on critical infrastructure are entirely possible and not merely the imaginings of worst-case scenario doomsayers. From events such as the Stuxnet attack it is also clear that destructive CNAs are complex, multi-stage operations. Analysts have concluded that the Stuxnet attack featured many of the attributes of conventional military operations including intelligence operations and mid-operation fragmentary orders. The attack involved a significant reconnaissance effort, likely including earlier intrusions into target systems.[51] Intelligence details that would have been useful to CNA operations such as Stuxnet include physical configuration of hardware, Internet Protocol addresses of connected computers, security patch installation histories, target platform operating systems, operator identities, and information on delivery of computer components to the target facility.[52] As noted above, rather than simply operating as off-the-shelf code, Stuxnet appears to have been designed, updated and even manipulated by it operators during the attack. It also appears the operation was monitored and commanded while in progress as are conventional, kinetic military operations.

43 In May 2010, the United States Department of Defense activated the U.S. Cyber Command, a military organization devoted to cyber operations. See Ellen Nakashima, *Gates Creates Cyber0Defense Command*, Washington Post, Jun. 24, 2009, at http://www.washingtonpost.com/wpdyn/content/article/2009/06/23/AR2009062303492.html.

44 David E. Sanger, *Iran Fights Malware Attacking Computers*, New York Times (Sep. 26, 2010).

45 Nicolas Falliere, et al., *W32.Stuxnet Dossier, Version 1.3*, Symantec Security Response, 1-2 (Nov. 2010) [hereinafter Falliere et al.].

46 *Id*. at 21.

47 *Id*.

48 *Id*.

49 David E. Sanger, *America's Dearly Dynamics With Iran*, New York Times (Nov. 6, 2011).

50 Mahnaimi, *supra* note 39.

51 Falliere, et al., *supra* note 44, at 3.

52 *See* Nat'l Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 118 (William A. Owens, Kenneth W. Dam, Herbert S. Lin eds., 2009).

In cyber operations parlance, intelligence collection and cyber reconnaissance or computer network exploitation (CNE) are often distinguished from CNA.[53] Analyzed independently, intelligence functions and CNE, such as those performed in support of Stuxnet, likely do not rise to the level of attack. Yet understood in context, many CNE could be understood as essential sub-components of an operation constituting an attack. CNE conducted immediately prior to an attack or even concurrently with an operation to damage or destroy property, such as appears to have been the case in the Stuxnet operation, present a strong case for satisfying logical and legal thresholds of attack. In law-of-war parlance, though not independently qualifying as attacks, CNE may nonetheless be said to constitute "direct participation in hostilities" – a function traditionally reserved to the combatant class. Thus questions arise concerning who might permissibly conduct CNE and even weapon design in support of CNA. Would the use of persons not meeting the four 1874 criteria described above warrant denial of combatant status and the consequences of combatancy? And would a State employing civilians to perform the intelligence functions, attack execution, or any of the other operations essential to a successful destructive CNA such as Stuxnet be in violation of the law of war?

The traditional and presently the majority answer is "yes." Respected international legal scholars have applied the 1874 criteria of combatant status to evaluate the question of lawful participation in cyber warfare. Nearly all conclude that only members of armed forces or organizations meeting the four 1874 criteria for combatant status should be employed to carry out CNA.[54] Most prescribe that States incorporate their cyber warriors into the regular armed forces or confer on them some military status. Few if any scholars or practitioners have deemed the 1874 inadequate or inapposite to the cyber context. Even scholars advocating innovative approaches to evaluating lawful participation in hostilities hew towards or even incorporate the four 1874 combatant status criteria.[55]

Yet, as I have suggested previously, several factors counsel skepticism towards unquestioning reliance on the 1874 criteria to evaluate combatant status in cyber warfare. First, States may already have heavily incorporated civilians into the agencies that support and conduct CNA on their behalf, making their direct participation in CNA likely if not certain. While the staffing details of States cyber war apparatuses are not publicly available, the executive mandates of several U.S. agencies suggest involvement in response to and use of CNA. In addition to the Department of Defense and its subordinate intelligence agencies (staffed in significant part

53 Computer network exploitation (CNE) refers to efforts to penetrate systems to gain information on the system and its vulnerabilities, thus acting as a tool for intelligence collection rather than system destruction. *See* Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues 5* (Cong. Research Serv., CRS Report for Congress Order Code RL31787, Mar. 20, 2007), available at http://www.fas.org/sgp/crs/natsec/RL31787.pdf.

54 *See e.g.* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 Harvard International Law Journal 179, 187 (2006); Adam Sherman, *Forward unto the Digital Breach: Exploring the Legal Status of Tomorrow's High-Tech Warriors*, 5 Chicago Journal of International Law 335, 339–40 (2004); Louise Doswald-Beck, *Computer Network Attack and the International Law of Armed Conflict*, in 76 International Legal Studies: Computer Network Attack and International Law (Michael N. Schmitt & Brian T. O'Donnell eds., 2002)(concluding that rules guiding combatant classification and privilege should be no different in CNA); Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, in Computer Network Attack and International Law (Michael N. Schmitt & Brian T. O'Donnell eds., 2002)(concluding that civilians participating in CNAs that actually or foreseeably result in injury, death, damage, or destruction would be illegal combatants).

55 *See* Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 National Security Law & Policy 257 (2008).

by civilian personnel), the U.S. Department of Homeland Security, the Central Intelligence Agency, and the Federal Bureau of Investigation share responsibility for defending against and responding to national security threats such as CNA.[56] Furthermore, the nature of both the physical and human capital of cyber warfare suggests a strong likelihood of significant civilian involvement. The programming expertise and vast network infrastructure of the civilian community and private sector make incorporation of their efforts into CNA seemingly irresistible.[57] Few, if any, of the actors holding the requisite expertise qualify as combatants under the 1874 criteria, thus rendering likely or even extant State practice inconsistent with presently conceived international law.

In addition to better aligning law and State practice, abandoning rote application of the 1874 combatant criteria accounts for their reduced practical relevance in cyberspace. First, although it is a significant indication of State affiliation or imprimatur, a criterion I will recommend be retained, the command criterion itself is a formalistic and empty requirement in cyber warfare. While the command requirement excludes individual actors and therefore preserves the collective nature of war, command remains essential in only a loose sense to cyberspace. Unlike their kinetic counterparts, cyber combatants are not typically isolated or removed from supervision or political leadership. The actions of cyber combatants seem susceptible to any number of management and supervision schemes including civilian or administrative oversight. In cyber warfare, requiring strict or formal military command is not uniquely suited to maintaining accountability or control of personnel carrying out CNA. If preserved as a prerequisite to combatant status in cyberspace, subordination to military command might easily be reduced to empty formalism – simply a paper drill conferring military status or bureaucratically incorporating what remains for all intent and purpose a civilian organization into an ersatz armed force of the State. Such hollow, *pro forma* measures would accomplish little, if anything, practically and would inevitably reduce respect for any law understood to require such steps.

The nature and circumstances of cyber warfare also undermine traditional application the second and third of the 1874 Brussels Declaration combatant status criteria. Because CNA constitute truly remote, over-the-horizon engagements, the classic requirements of distinctive insignia and carrying arms openly are of greatly reduced utility. Visually, cyber warriors are extremely unlikely to confront their foes. Unlike conventional kinetic attack, where attackers select targets on the basis of outward appearances or where defenders respond to the appearance of persons conducting the attack, CNA targets are selected on the basis of functionality or informational value. Far more than the outward appearance of individuals conducting CNA, 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.

The final requirement of the 1874 criteria, that combatants' operations comply with the law of war enforceable through an internal disciplinary system retains much of its force but nonetheless takes on relatively reduced significance as well in CNA. While this fourth criterion undoubtedly

56 Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 app. at 542–51 (2006).

57 *See* Susan W. Brenner, Cyberthreats: The emerging Fault Lines of the Nation State (2009) (arguing for better integration of civilian law enforcement and intelligence organizations and military response to cyber attacks); Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 Vanderbilt Journal of Transnational Law 1011 (2010); Susan W. Brenner & Leo L. Clarke, Civilians in Cyberwarfare: Casualties, 13 Southern Methodist University Science & Technology Law Review 249 (2010).

retains its normative appeal and humanitarian effect with respect to observance of the law of war, the requirement of an internal disciplinary system one finds in later expressions of the fourth criterion seems largely inapposite to CNA. Envisioned as portable justice mechanisms capable of following armed forces wherever they operate and overcoming jurisdictional defects of their civilian counterparts, internal, military justice systems were a necessary corollary to command. Military justice was essential to enforcing discipline and preventing lawless exploitation of the battlefield by super-empowered belligerents. CNAs rarely, if ever, call for such jurisdictional portability and insularity. Participants in CNA need not be geographically displaced from civilian municipal justice systems. While investigating and prosecuting cyber war crimes would undoubtedly present great technical and legal challenges, the challenges specific to the kinetic battlefield deployment seem not to carry over in sufficient scale to warrant subjection to an internal military disciplinary system as a criterion for combatant status. In fact, the law of war increasingly forms part of States' domestic criminal codes, permitting meaningful civilian prosecution of war crimes committed by cyber warriors.[58] Finally, because senior leaders and legal advisors, presumably better-steeped in the law of war, can position themselves literally at arm's length from subordinate cyber combatants, the need for fourth criterion overall is perhaps reduced.

In contrast to the four 1874 Brussels Declaration criteria for combatant status, the single criterion of State affiliation far better supports the likely future of State practice in cyber warfare and vindicates the still important normative goals of the law of war. First, State affiliation preserves concern for the principle of distinction in CNA. If concern for distinction persists in cyber warfare, concern lies not so much with the identities and appearances of participants in CNA as much as with their weapons and the appearances generated by the attack itself. CNA have great capacity to confound their targets. Thus, the true challenge from CNA with respect to distinction may result not from civilian participation, rather from efforts to disguise the true source of the attack. CNA routed through civilian servers or programmed to appear as though they originated from civilian institutions may in fact run afoul of states' duty to bear arms openly in the attack. Exploration of this aspect of CNA's relation to distinction, however, is better left to a dedicated legal discussion of means and methods in CNA.

While considerable clarification of distinction in the context of CNA is required, state affiliation ensures that attacks remain subject to the existing international legal framework. In particular, the war crime of perfidy may present a more effective check against CNA exploiting peaceful or civilian networks as cover than restricting combatant status. Examining distinction, specifically the duty for those taking a direct part in hostilities to make themselves distinct from civilians, civilian CNA participants do not fail distinction by virtue of intentional perfidy. The intent of States' use of civilians in CNA is not to take advantage of enemy forbearance in targeting such civilians. More likely economic, training, and recruitment limitations drive the use of civilians in CNA. Situated far from the battlefield, if cyber warfare can be said to have a battlefield,[59] civilians participating in CNA do not present a confused picture to the enemy from the perspective of distinction. The likelihood that state-sponsored CNA could be misattributed

58 International Committee of the Red Cross, *International Humanitarian Law National Implementation Database, available at* http://www.icrc.org/ihl-nat.nsf/WebALL!OpenView (providing State-by-State information on domestic implementation of the law of war).

59 *See* Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 Yale Hum. Rts. & Dev. L.J. 143, 161–62 (1999). Battlespace describes both "virtual and non-linear loci of combat." *Id*. at 161.

to innocent civilian assets and systems make distinction of means far more important than distinction of personnel launching attacks.

In addition, reliance on state affiliation as the sole criterion for lawful participation in CNA presents no greater threat to discipline in warfare. While civilians participating in CNA are ordinarily not subject to internal military disciplinary systems, the increasing well-developed legal regimes that prosecute and punish war crimes operate nonetheless and vindicate concerns for discipline and humanity. As outlined above, when adopted by the 1949 Convention the criterion of exposure to an internal disciplinary system as a precondition to combatant status seemed reasonable. International enforcement bodies such as the International Criminal Court did not exist. Moreover, the international community's political will to convene *ad hoc* tribunals to prosecute war crimes appeared spotty and susceptible to victor's bias. Few if any international war crimes enjoyed domestic implementation or incorporation into states' domestic criminal codes. What enforcement of war crimes law existed was constrained largely to members of armed forces. The wide-scale incorporation of the law of war into domestic criminal mechanisms where civilians are equally susceptible to war crimes prosecution, including forms of vicarious liability, mitigates concerns that merely requiring State affiliation would inadequately serve the important concern of combatant discipline and humanity.

4. CONCLUSION

> *"The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas."*[60]

Like other innovations in warfare, cyber warfare will likely demand altered understandings of existing legal and operational precepts. While the principles and even many of the particulars of the law of war will in large part suffice to ensure a level of humanity and order in cyber warfare, to expect an unchanged or static legal convention to operate is unrealistic and would be ultimately self-defeating. As the above quotation makes clear, cyber hostilities will demand States issue clarifications and even operate under glosses on accepted tenets of the law of war.

The standards for combatant status in cyber warfare appear to be ripe for such a clarification. Recent developments including the Stuxnet attack make clear that executing successful CNA will place intense demands on States' human and technical capital, inducing many to resort to segments of their civilian population's expertise and infrastructure. Given the important consequences of determinations of combatant status, the extent to which the law of war accepts or condemns States' resort to their technical and personal capital may be one of the most important legal questions surrounding cyber warfare.

60 *Cyberspace Policy Report, supra* note 42, at 7-8.

Well-suited to the battlefields they imagined and those of over 100 years of succeeding armed conflicts, the 1874 Brussels Declaration combatant criteria continue to perform a useful sorting function on kinetic battlefields pitting visible adversaries against one another. The important principles of distinction and discipline draw direct support for each of the four criteria. Yet transposed to the realm of cyber warfare and use to evaluate the propriety of participation in hostilities by cyber warriors, the 1874 criteria appear dated and detached. Mainstream legal scholarship on combatancy in cyber warfare would exclude many cyber warriors from the class of lawful combatant unnecessarily and likely to the great disruption of existing or planned State practice while achieving little payout with respect to humanitarian ideals. Secondary rules, such as the proposed State affiliation gloss on the requirements of combatant status will both take account of emerging State practice while supporting the critically important notion captured in the primary rule of distinguishing combatants from civilians.

Idealized portraits of war are not entirely fatuous. Capturing our highest humanitarian aspirations in international law at once testifies to our shared interest in shielding the innocent and stricken from the horrors of war and reveals our belief in the power of law to work for good, even in the face of war. Yet alongside these aspirations must operate realistic and pragmatic understandings of the limits of combatants' capabilities and characteristics. Such understandings and interpretations secure law's voice in war and build the confidence in its end users necessary for its further development and efficacy.