INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

Cyber Warriors and the *Jus in Bello*

Vijay M. Padmanabhan

89 INT'L L. STUD. 288 (2013)

Volume 89 2013

Cyber Warriors and the *Jus in Bello*

Vijay M. Padmanabhan[*]

I. INTRODUCTION

The increasing interest in cyber operations, or "efforts to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them,"[1] as a warfighting tool raises questions regarding application of the *jus in bello* to "cyber warriors," or actors involved with cyber operations. Most cyber warriors will not be evaluated under the law of armed conflict. Cyber operations to date generally have amounted to nothing more than annoyances or crimes, or were in reality espionage, and therefore are regulated by municipal criminal law.[2] Where there is an armed conflict, most cyber operations and responses to cyber operations target

* Assistant Professor, Vanderbilt University Law School. Thanks to Ashley Deeks, Andy Grotto and Mike Newton for their helpful comments on this project.

1. *See* Matthew C. Waxman, *Cyber Attacks as "Force" under U.N. Charter Article 2(4)*, *in* INTERNATIONAL LAW AND CHANGING CHARACTER OF WAR 43 (Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies) (defining "cyber-operations").

2. *See* James A. Lewis, *Cyber Attacks, Real or Imagined, and Cyber War*, CSIS (July 11, 2011), http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war (arguing against "hyperbole" in characterizing cyber operations as acts of war).

infrastructure and property, thereby bypassing the rules governing targeting of persons.

Nevertheless, the question of the legal status of cyber warriors under the *jus in bello* is likely to arise in two circumstances. First, the international armed conflicts and non-international armed conflicts of the present and the future are likely to include cyber operations as one element of an integrated war strategy. The 2008 armed conflict between Russia and Georgia over South Ossetia included large-scale distributed denial of service (DDS) attacks against Georgian government websites in an effort disrupt communication between the government and its people.[3] The relatively low cost of cyber operations compared to kinetic attacks suggests they are likely to be used, perhaps in more destructive ways, in future wars.[4]

Second, an isolated cyber operation may have sufficient kinetic effects to rise to the level of an "armed attack," justifying the use of force in lawful self-defense. The United States and Israel launched a cyber operation against Iran's burgeoning nuclear program that used malicious code to impede the functioning of Iran's centrifuges in order to secure additional time for negotiations over the future of Iran's nuclear capability.[5] This operation, code-named Olympic Games, led at least one scholar to argue that the United States and Israel committed an armed attack against Iran.[6] It is reasonable to assume that States may wish to use force in the future against those involved in such attacks, and indeed the United States has expressly reserved the right to do so.[7] Such force may amount to an "armed conflict" under the *jus in bello*, thereby raising issues as to the status of those targeted.

Under these two circumstances, categorization of cyber warriors as combatants, civilians or potentially unlawful combatants carries consequences. The most important of these are with respect to targeting. Com-

---

3. *See* John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES, Aug. 13, 2008, at A1 (describing attacks).

4. *See id.* (quoting expert comparing the low cost of cyber operations to the greater cost of kinetic operations).

5. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (describing details of the Olympic Games program).

6. *See, e.g.,* Paul Rosenzweig, *The Stuxnet Story and Some Interesting Questions,* LAWFARE BLOG (June 2, 2012, 16:52 EDT), http://www.lawfareblog.com/2012/06/the-stuxnet-story-and-some-interesting-questions/ (arguing Olympic Games amounted to an "armed attack" against Iran as understood under the U.N. Charter).

7. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 14 (2011) (reserving the right to use "all necessary means," including military force, to defend the United States and its allies from cyber operations).

batants, lawful or unlawful, are subject to targeting at all times during an armed conflict by virtue of their status. Civilians, by contrast, may not be made the object of attack,[8] except for such time as they directly participate in hostilities.[9] Civilians present during an attack also must be accounted for in the attacker's proportionality analysis, unless they are directly participating.[10] Consequences also arise with respect to the detention, treatment and prosecution of cyber warriors,[11] although their capture by the enemy is relatively unlikely.[12]

This article analyzes the difficult legal questions raised by application of the *jus in bello* categories to cyber warriors. The traditional category approach to targeting and detention works best when participation is limited to traditional combatants and it is possible to distinguish on the battlefield between combatants and civilians. Both assumptions are challenged in cyber operations.

First, actors other than traditional combatants are likely to play a significant role in cyber operations. The complex nature of cyber weapons may

---

8. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(2), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

9. *Id.*, art. 51(3).

10. *See id.,* art. 57(2)(b) (introducing the requirement of "proportionality").

11. Captured combatants may be detained until the end of hostilities. Lawful combatants enjoy immunity from prosecution in the national courts of the enemy State for actions undertaken consistent with the laws of war, and are entitled to prisoner of war privileges after capture. Knut Dörmann, *The Legal Situation of "Unlawful/Unprivileged Combatants,"* 85 INTERNATIONAL REVIEW OF THE RED CROSS 45, 45–46 (2003). Unlawful combatants, if the category exists, differ from lawful combatants in that they lack combatant immunity and are not entitled to prisoner of war privileges. Civilians, as "protected persons," by contrast may only be detained on the basis of an individualized determination that the security of the detaining power makes detention absolutely necessary, and it must cease when the need ends. Convention Relative to the Treatment of Civilian Persons in Time of War art. 42–43, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 31 [hereinafter GCIV]. Civilians are not entitled to prisoner of war privileges, and may be subject to prosecution in a capturing State's civilian courts based upon activities for which a combatant would be immune.

12. Physical capture of a cyber warrior will take place only if: (1) the individual is present within the attacked State or territory occupied by that State; (2) is captured as part of a military operation in another State; or (3) is brought within the jurisdiction of the attacked State through legal means, such as extradition, or unlawful means such as rendition. Capture is most likely where the cyber warrior acts independently or on behalf of a non-State actor such that the State where he is located will participate, cooperate or acquiesce with capture. Capture is exceedingly unlikely where the cyber warrior acts on behalf of a State engaged in an armed conflict and directs his attacks from that State.

result in States using contractors with technical expertise to modify continually the features of the weapon in order to overcome the defenses of the target, blurring the line between the traditional civilian task of weapons development and the traditional combatant task of weapons use.[13] In other instances, States may see an advantage in using non-State actors to launch cyber operations on their behalf in order to retain plausible deniability with respect to its role in the attack.[14] Civilians may also play an active role in defending critical networks against cyber operations, given that many attacks will be against dual-use infrastructure managed by civilians.[15]

Actors with no links to any State may become cyber warriors, either through participating in a cyber operation on behalf of an organized armed group involved in non-international armed conflict, or on their own due to sympathies for a belligerent. The reduced financial resources required for cyber operations compared to traditional kinetic operations of similar strength makes it more feasible for non-State actors to employ such operations.[16]

Second, it is harder to determine what particular role an individual plays in cyber operations as compared to traditional military operations. Cyber operations are potentially difficult to trace given the risk that they will utilize the infrastructure of unsuspecting third parties to mask their involvement.[17] Even if the attacks are traced to a particular State or organization,

---

13. *See* Sean Watts, *Combatant Status and Computer Network Attack*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 392, 409–10 (2010) (describing the need for continuous technical expertise in deployment of cyber weapons). The problems posed by contractors assuming traditional combat roles are not unique to cyber and have been discussed elsewhere in the literature.

14. *See* Gregory J. Rattray & Jason Healey, *Non-State Actors and Cyber-Conflict*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 67, 73 (Kristin M. Lord & Travis Sharp eds., 2011) (speculating that Iran might use Hezbollah to launch cyber operations to avoid attribution to Iran).

15. Congress has recently been involved in an extensive debate regarding the role of private actors in defending U.S. information infrastructure from cyber operations. *See* Michael S. Schmidt, *Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster*, NEW YORK TIMES, Aug. 2, 2012, at A3 (describing disagreement over cybersecurity standards for cooperation between corporations and the government).

16. *See* Rattray & Healey, *supra* note 14, at 67 (arguing that there is tremendous potential for non-State actors to use cyber attacks).

17. This problem has attracted attention in the context of the *jus ad bellum*, where attribution is required in order to invoke the right of self-defense. *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 443–44 (2011) (describing the effect of technical attribution problems on development of refinements to *jus ad bellum*).

resolving "doubt" as to whether the individual involved in the operation is targetable will be difficult to do.[18]

As a result, existing law provides at best imperfect guidance on targeting and, where relevant, detention decisions. While at least one scholar has suggested that these limitations with existing law demonstrate the need for an international "cyberspace treaty,"[19] the limited understand of the potential of cyber operations, the differing agendas of international actors on cyber questions and the contested nature of the legal issues all render completion of such a treaty highly unlikely. Instead, informal partnerships between like-minded States to develop joint strategies to handle cyber warriors may begin the process of developing new, more detailed rules regulating cyberspace.

II. LAWFUL COMBATANTS

Some subset of cyber warriors will qualify as lawful combatants subject to targeting at all times during an armed conflict and detention until the end of hostilities, but with the protection of combatant immunity and prisoner of war privileges if captured. These cyber warriors are formally integrated into the armed forces of a State under the domestic law of that State.[20] Their formal membership within the armed forces renders them non-civilians irrespective of their particular function with respect to the cyber operation.[21] Thus, the small cyber unit within United States Strategic Command involved in the Olympic Games attack would be composed of lawful combatants in an armed conflict with Iran, regardless of the particular function of any member of the unit with respect to the operation.[22]

---

18. *See* Additional Protocol I, *supra* note 8, art. 50(1) ("In case of doubt whether a person is a civilian, that person shall be considered to be a civilian."); art 52(3) (In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.").

19. Rex Hughes, *A Treaty for Cyberspace*, 86 INTERNATIONAL AFFAIRS 523, 524 (2010).

20. Additional Protocol I, *supra* note 8, arts. 43(1) & 44(1); Convention Relative to the Treatment of Prisoners of War art. 4(a)(1), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GCIII].

21. *See* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES 25 (2009) ("Members of regularly constituted forces are not civilians, regardless of their individual conduct or the function they assume within the armed forces.").

22. Article 46 of Additional Protocol I excludes members of the armed forces engaging in espionage from prisoner of war status. Such exclusion is potentially important to

But, as explained at the outset, States may employ in cyber operations at least three categories of actors who are not formally affiliated with the armed forces of the State. States may hire civilian contractors to design weapons that will be employed in a cyber operation.[23] While weapons design has traditionally been viewed as a civilian activity, cyber weapons are different from tanks or planes in that the weapon must itself be modified continuously to react to unexpected and evolving defenses within a specific target.[24] Such modifications require weapons designers to work much more directly with military and intelligence counterparts during the course of the attack, increasing the quality and intensity of their participation in the conflict.[25]

Second, States may use non-State actors to launch cyber operations in order to maintain plausible deniability for state responsibility purposes. For example, the Georgian government accused the Russian Federation of hiring criminal organizations and encouraging patriotic "hacktivists" to launch attacks against Georgia during the 2008 conflict over South Ossetia.[26]

Third, States may rely upon members of its civilian population to defend civilian infrastructure from incoming cyber operations. States increasingly rely upon private assets, such as fiber optics networks, Internet service providers and commercial data storage facilities, as dual-use infrastructure.[27] These assets can be targeted in cyber operations, placing the civilian ownership of these networks at the front lines of any defense effort. Such defense may be purely reactive, as the network operators merely try to mit-

---

cyber warriors because many cyber operations are accompanied by espionage. If captured by the enemy in an armed conflict, members of the armed forces engaged in espionage might not receive prisoner of war privileges and may be prosecuted. However, the military advantage of cyber espionage is that it can be conducted remotely, outside the territory of the spied upon State. Under such circumstances, the capture of a spying cyber warrior is unlikely. The loss of prisoner of war privileges is irrelevant to the right of the aggrieved State to target a spying member of the armed forces as part of an armed conflict.

23. Such contractors risk mercenary status if they are not nationals of the State, are motivated to participate in the conflict by desire for pecuniary gain and are paid compensation substantially in excess of that received by members of their armed forces of a similar rank. *See* Additional Protocol I, *supra* note 8, art. 47 (detailing requirements for mercenary status).

24. Watts, *supra* note 13, at 409–10.

25. *Id.* at 410.

26. *See id.* at 411 (quoting the chief of the Georgian National Security Council).

27. *See* Rattray & Healey, *supra* note 14, at 67 (explaining why non-State actors are likely to play an outsized role in cyber defense).

igate the effects of the attack.[28] But in other instances, those under attack may choose to counterstrike in an effort to end the attacks. Such an offensive response to attacks might be the cyber equivalent of traditional partisans taking up arms to protect their country in response to a kinetic attack.[29]

Such actors could be recognized as lawful combatants under the Third Geneva Convention.[30] Article 4(A)(2) provides that members of other militias "belonging to a Party to the conflict" are lawful combatants entitled to prisoner of war privileges provided that they are under responsible command, observe the principle of distinction by wearing a fixed sign and carrying arms openly, and conduct their operations consistent with the laws and customs of war. Cyber warriors involved in the design and launch of cyber weapons, as well as quasi-independent groups used to launch cyber operations, could conceivably meet these requirements.

Article 4(A)(6) grants inhabitants of a non-occupied territory prisoner of war status if they spontaneously take up arms to defend against invading forces, if they carry arms openly and respect the laws and customs of war. Civilians administering critical infrastructure who use active defenses to respond to a cyber operation might be categorized as a cyber *levée en masse*, and thereby entitled to combatant status.

Nevertheless, two difficulties exist with applying these provisions to cyber warriors. First, to qualify for lawful combatant status under Article 4(A)(2) the group in question must "belong to a Party to the conflict." The ICRC's *Interpretive Guidance* on direct participation in hostilities concludes that this standard is satisfied by a de facto relationship between the State and the group such that it is evident that the group conducts hostilities "on behalf and with the agreement of the Party."[31]

The International Criminal Tribunal for the former Yugoslavia Appeals Chamber in the *Tadić* case held that a State must exercise "effective control" over such a group for it to "belong to" the State. Effective control requires a relationship of "dependence and allegiance" with the State.[32] If

28. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 1011, 1032–33 (2010).

29. *See id.* at 1033–35 (explaining why such an outcome may be more likely in the cyber realm).

30. GCIII, *supra* note 20.

31. MELZER, *supra* note 21, at 23.

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

the State is using such a group to launch cyber operations to avoid State responsibility, then it may be very difficult to locate evidence to establish that the group is, in fact, acting under the "effective control" of the State.

Second, both 4(A)(2) and 4(A)(6) demand that lawful combatants abide by the principle of distinction, whether by wearing a fixed sign and/or carrying arms openly.[33] Literal application of these requirements to cyber warriors is likely to result in the conclusion that some of these actors are not lawful combatants. They are unlikely to wear uniforms, given that they are not part of the armed forces of the State. They are also likely to hide the military nature of computers used in a cyber operation by employing the outward markings of civilian computer infrastructure, such as a civilian Internet Protocol (IP) address.

Scholars have argued that these distinction requirements are antiquated with respect to cyber operations because cyber operations are launched remotely; the failure of a cyber warrior to wear a uniform, for example, does not provide him an inappropriate military advantage by appearing to blend with the civilian population.[34] Heather Dinniss writes that a potential update to these provisions in the context of cyber would be to mandate that cyber operations be launched from a computer with a military IP address in order for the cyber warrior to receive combatant status.[35] She questions, however, the practicality of such a requirement, explaining that a military IP address would place an immediate target on the computer involved in an attack.[36]

Query, however, whether this result is any different from the target a soldier in a traditional conflict places on himself by wearing a uniform and carrying his arms openly. A requirement that in order to be a lawful com-

33. There is a vigorous legal debate about whether these requirements must be met by regular armed forces as well in order to qualify as lawful combatants. *Compare* Sean D. Murphy, *Evolving Geneva Convention Paradigms in the War on Terrorism: Applying the Core Rules to the Release of Persons Deemed "Unprivileged Combatants,"* 75 GEORGE WASHINGTON LAW REVIEW 1105, 1127–28 (2007) (arguing yes), *with* Evan J. Wallach, *Afghanistan, Quirin and Uchiyama: Does the Sauce Suit the Gander?*, 2003 ARMY LAWYER, Nov. 2003, at 18, 24 (arguing no).

34. *See* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 145 (2012) (describing usefulness of literal application of requirements of having a fixed distinctive sign recognizable at a distance and carrying arms openly as "diminished" with remote attacks); Watts, *supra* note 13, at 440 (same).

35. DINNISS, *supra* note 34, at 146.

36. *Id.* ("requiring a computer to be marked as a military computer is tantamount to painting a bulls-eye").

batant a cyber warrior must use a military IP address in his attacks incentivizes transparency in cyber operations. Transparency mitigates the risk that an attacked State would retaliate against a third State or civilian infrastructure not actually involved in a cyber operation because of a false IP address.

III. CIVILIANS

The analysis in Part II suggests that some subset of cyber warriors with an affiliation or sympathy toward a State in an armed conflict may not be lawful combatants. There are other similarly situated cyber warriors.

Cyber warriors engaged in cyber operations on behalf of non-State groups which are engaged in non-international armed conflict are not to be entitled to lawful combatant status because they do not "belong to" a State party to the conflict. For example, members of al Qaida have admitted to engaging in "low-level and disruptive" cyber operations including sabotage of political websites and denial of service attacks as part of their organization's war with the United States.[37] Such individuals, even if part of the armed wing of al Qaida, would not qualify for lawful combatant status.

"Hacktivists," or non-State actors unaffiliated with either side in an armed conflict who undertake cyber operations out of personal sympathies with a belligerent also do not qualify for combatant status because they lack a relationship with a State party to the conflict. One explanation for the DDS attacks directed against Georgian websites is that they were launched by the nationalist Russian hacker community, which may have been tipped off by the Russian government about plans to use force in South Ossetia.[38] Such a loose affiliation with the State is unlikely to meet the standard for "belonging to a Party" to the conflict because hacktivists are not under the "effective control" of the State.

Some scholars[39] and the Israeli Supreme Court[40] have taken the position that anyone who is not a lawful combatant is a civilian. The Interna-

37. *See* Rattray & Healey, *supra* note 14, at 72 (quoting statements of Guantanamo detainee Mohamedou Ould Slahi describing al Qaida's cyber capabilities).

38. *See* PAUL CORNISH ET AL., CHATHAM HOUSE, ON CYBER WARFARE 6 (2010) (detailing attacks by private Russian groups on Georgia and Estonia).

39. *See, e.g.,* Marco Sassòli, *Use and Abuse of the Laws of War in the "War on Terrorism,"* 22 LAW & INEQUALITY 195, 207–08 (2004) (listing scholarly support for this position).

40. *See* HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006(2) PD 459, ¶ 28 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS

tional Committee for the Red Cross (ICRC) *Commentary* on Geneva Convention IV (GCIV) indicates that it was the intention of the drafters of the Geneva Conventions to cover everyone within the ambit of the treaties, either as a prisoner of war or as a civilian.[41] Such a view draws support from the text of GCIV, which does not expressly exclude those engaged in fighting from protected person status and does contemplate "spies and saboteurs" achieving that status in occupied territory.[42]

If cyber warriors are civilians, they would be subject to targeting only "for such time as" they "directly participate in hostilities."[43] The content of the direct participation standard is the subject of significant legal debate. The ICRC issued *Interpretive Guidance* on the content of the terms,[44] which in turn has spawned numerous scholarly critiques of both the process by which the *Guidance* was created and its content.[45] Nevertheless, it is useful to consider some of the challenges in applying the components of direct participation identified by the ICRC to cyber warriors in an effort to understand what may be at stake in categorizing them as civilians.[46]

The *Interpretive Guidance* provides that a civilian directly participates in hostilities when he (1) engages in an act that directly causes (2) harm of a

373 (2007) (treating Palestinian militants as civilians because it did not see a basis for recognizing a category other than lawful combatant and civilian).

41. *See* COMMENTARY: IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PROTECTED PERSONS IN TIME OF WAR 51 (Jean S. Pictet ed., 1960) [hereinafter FOURTH GENEVA CONVENTION COMMENTARY] ("Every person in the hands of the enemy must have some status under international law."). In addition to prisoner of war and civilian, Pictet explained that an individual could also be protected under the First Geneva Convention as medical personnel. *Id.*

42. GCIV, *supra* note 11, art. 5. *See also* FOURTH GENEVA CONVENTION COMMENTARY, *id.* at 53 (defending the need to provide spies and saboteurs "protected person" protections).

43. Additional Protocol I, *supra* note 8, art. 51(3).

44. MELZER, *supra* note 21.

45. *See generally* Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 637 (2010) (summarizing a range of perspectives on the *Interpretive Guidance*).

46. Categorizing cyber warriors as civilians also has consequences for detention. Civilian protected persons may be detained only for imperative reasons of security, unlike combatants who may be detained for the duration of hostilities without individualized reason. *See* GCIV, *supra* note 11, art. 42 (permitting detention of civilians when demanded by security). But as discussed above, cyber warriors are unlikely to be detained under the laws of war given the difficulties inherent in their capture, and therefore this article focuses on consequences for targeting.

sufficient gravity with (3) the intent of aiding a belligerent party. Application of each of these terms to cyber warriors raises difficult legal questions.

The ICRC argues "direct causation" is satisfied where the participation in question causes the requisite level of harm in "one causal step."[47] Such a requirement distinguishes between acts like scientific research and weapons design, which require further action to bring the harm to fruition and are not direct participation, and the deployment of weapons themselves, which causes the harm in question, and is direct participation.[48]

The "direct causation" requirement appears easier to meet in the context of cyber operations than in traditional kinetic operations. Cyber weapons by their nature require constant modifications to overcome the active defenses of the target. As a result, those designing weapons may be called upon to operationalize their weapon, using intelligence about the target to do so.[49] The increased depth and quality of such participation may meet the "direct causation" standard because the act of modifying cyber weapons during the course of an operation to overcome system defenses is "one causal step" away from the harm in question. Indeed, the *Interpretive Guidance* explains that production of weapons "carried out as an integral part of a specific military operation" meets the causation requirement.[50]

Such an outcome raises concerns from the perspective of those favoring a more robust role for human rights protections in warfighting. One concern raised about the ICRC *Guidance* is that it defines direct participation too broadly, in the process opening up too many civilians to the use of force.[51] To the extent cyber warriors blur the line between combatant and civilian and are therefore subject to targeting, these worries are exacerbated.

The "threshold of harm" limits direct participation to acts that either are likely to affect the military operations or military capacity of a party to an armed conflict, or which result in death or injury to civilians or destruction of civilian property. The ICRC *Guidance* specifically states that attacks on the computer networks of the military can be sufficiently grave to con-

---

47. MELZER, *supra* note 21, at 53.

48. *See id.* (distinguishing general design and transport of weapons from their use in specific military operations).

49. *See* Watts, *supra* note 13, at 410 (claiming civilians "are likely to participate in a more direct and ongoing fashion" with cyber weapons).

50. MELZER, *supra* note 21, at 53.

51. *See* Goodman & Jinks, *supra* note 45, at 639 (describing concerns of human rights actors with the ICRC *Guidance*).

stitute direct participation.[52] But the *Guidance* rejects the idea that "manipulation" of civilian computer networks passes the threshold of harm requirement, unless the result is destruction of civilian infrastructure.[53]

The threshold of harm standard has the potential to distinguish between the participation of different categories of cyber warriors. Cyber warriors involved in exploitation of military and government systems to obtain tactical intelligence information or destroy military infrastructure will see their acts pass the requisite threshold of harm, and thus be subject to targeting provided the remaining criteria are met. By contrast, those exploiting civilian systems for the purpose of harming the economic prospects of an enemy State would likely not meet the threshold of harm, unless they destroy civilian infrastructure in the process of doing so.

Michael Schmitt has criticized the threshold of harm standard for being "under-inclusive" in terms of the conduct included within the ambit of direct participation. Schmitt questions why the *Interpretive Guidance* limits participation to acts that cause "death, injury, or destruction" to civilians and civilian property, as opposed to including any harmful acts directed against protected persons and objects that are part of war strategy or are evidently related to ongoing hostilities.[54] Application of the threshold of harm standard to cyber warriors demonstrates the strength of these concerns. Cyber warriors are free to engage in cyber operations that could exact a significant toll on the civilian population of the enemy State without risk of being targeted, a consequence seemingly at odds with the goal of protecting civilians from the consequences of armed conflict.

The requirement of "belligerent nexus" requires that an act of direct participation be objectively intended to cause the requisite threshold of harm in aid of a party to a conflict. Such a requirement is designed in part to weed out unrelated but coterminous violence, such as a bank robbery in a war zone. In the context of cyber warriors the requirement would distinguish between patriotic hacktivists objectively seeking to aid their country

52. *Id.* at 48.

53. *See id.* at 50 (comparing manipulation of civilian computer networks to building fences or roadblocks, disrupting food or electrical supplies, appropriating property or arresting and deporting civilians).

54. Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 697, 724 (2010).

in war and groups like Anonymous[55] that may commit very similar attacks but with no intention to benefit belligerents.

This requirement may produce some unusual, and arguably inequitable, results when applied to cyber. Anonymous threatened to launch a cyber operation against the Pentagon over its continued detention of Private First Class Bradley Manning because of his involvement in the WikiLeaks affair.[56] If such an operation were launched by an al Qaida cyber unit as part of its armed conflict with the United States, then al Qaida warriors involved in the operation would meet the belligerent nexus requirement. By contrast, members of Anonymous, motivated by free speech concerns, would not, even if their attack would have similarly problematic consequences for the U.S. effort to combat al Qaida. Such disparate outcomes may be justifiable in the context of kinetic attacks, where States may have law enforcement options with respect to mitigating the threat posed by actors lacking requisite belligerent nexus. But such an outcome is harder to stomach in the cyber context, given that such attacks may emanate from outside the State, leaving States with few alternatives to force to mitigate the threat.

The direct participation standard also imposes temporal limitations on targeting civilians. Additional Protocol I permits targeting of directly participating civilians only "for such time" as they directly participate. What might this standard mean in the context of cyber? Consider that a State may not be aware of a cyber attack until long after the participation of any of the actors involved in the attack has terminated. Iran, for example, was not aware that the problems with its centrifuges were related to foreign sabotage until well into the Olympic Games program.[57] Strict interpretation of the "such time" language could well insulate civilians involved in programs like Olympic Games from targeting by States. The ICRC *Guidance* appears to endorse this result, stating "with computer network attacks . . . the duration of direct participation in hostilities will be restricted to the

---

55. Anonymous describes itself as "a decentralized network of individuals focused on promoting access to information, free speech, and transparency." *About Us*, ANONYMOUS ANALYTICS, http://anonanalytics.com/ (last visited Nov. 9, 2012). *See also* Scott Neuman, *Anonymous Comes Out in the Open*, NPR (Sept. 16, 2011, 5:02 PM), http://www.npr.org/2011/09/16/140539560/anonymous-comes-out-in-the-open (describing Anonymous as a "cyberguerilla" group).

56. *See* Michael Stone, *Pentagon Fears Anonymous Attack, re: WikiLeaks, Bradley Manning*, EXAMINER (Mar. 9, 2011), http://www.examiner.com/article/pentagon-fears-anonymous-attack-re-wikileaks-bradley-manning.

57. *See* Sanger, *supra* note 5 (describing initial reaction of Iranian officials to Stuxnet).

immediate execution of the act and preparatory measures forming an integral part of that act."[58]

Heather Dinniss suggests that the temporal duration of a cyber operation could include the time during which the effects of the cyber weapon are being felt. Dinniss explains such an interpretation is consistent with the nature of a cyber operation: the operation is ongoing as long as the cyber weapon is acting against the computer system of the enemy, much as a kidnapping goes on during the entire length a person is held hostage. This interpretation of the temporal limitations of the direct participation standard would better protect the ability of belligerents to target those involved in cyber operations that have a continuing adverse effect on military operations. It would also potentially discourage civilian participation, a core goal of international humanitarian law (IHL).

IV. UNLAWFUL COMBATANTS

There are, however, significant inequities that result from treating cyber warriors as civilians. Limiting targeting to such time as cyber warriors directly participate, and including them in a proportionality analysis gives such individuals greater protections from targeting than lawful combatants. Such a rule creates an incentive for cyber units to avoid following the distinction and attribution rules needed for lawful combatant status.[59] This perverse incentive is stronger in the cyber context than elsewhere because cyber warriors are unlikely to be captured, and therefore to need the combatant immunity and prisoner of war privileges that come with being labeled a lawful combatant. The inequities that result from treating irregular fighters as civilians explain the position of at least some States during the negotiations of the Fourth Geneva Convention against doing so.[60]

Instead, some scholars and States argue that international law recognizes a third category for targeting and detention purposes: "unlawful combat-

58. MELZER, *supra* note 21, at 68.

59. *See* Richard D. Rosen, *Targeting Enemy Forces in the War on Terror: Preserving Civilian Immunity*, 42 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 683, 736–39 (2009) (describing difficult consequences that result from treating non-State soldiers as civilians).

60. *See* 2 FINAL RECORD OF THE DIPLOMATIC CONFERENCE OF GENEVA OF 1949, sec. A, at 621 (1949) (quoting British delegate explaining "the whole conception of the Civilian Convention was the protection of civilian victims of war and not the protection of illegitimate bearers of arms").

ant" or "unprivileged belligerent."[61] Unlawful combatants are subject to targeting at all times as are lawful combatants.[62] They are also not included as collateral damage in the targeting proportionality determination. This categorization would eliminate an incentive for cyber warriors to avoid meeting the requirements for lawful combatant status.

Given the varied groups of cyber warriors described in Parts I and II who are not entitled to lawful combatant status, the category of unlawful combatant must distinguish between those who should be subject to targeting at all times during the armed conflict, and those who deserve the protections afforded civilians. Unfortunately, there is no agreed test within international law as to when an individual becomes an unlawful combatant. The debate over categorization of irregular fighters in the post-9/11 conflicts has led to debate over the potential boundaries for such a category.

The ICRC's *Interpretive Guidance* categorizes those whose "continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation" as combatants.[63] It would distinguish these individuals from "recruiters, trainers, financiers and propagandists," who contribute to the war effort, but in a manner more akin to civilian supporters than combatants.[64]

Of most interest in the context of cyber operations is that the *Guidance* considers the purchase, manufacturing and maintenance of weapons outside of a specific military operation, as well as the collection of intelligence that is not tactical in nature, to be civilian functions. Under this approach categorizing cyber warriors would turn largely on whether they have regu-

---

61. This was the approach taken by the Bush administration to categorize members of the Taliban and al Qaida in the post-9/11 conflicts. Memorandum from President George W. Bush to the Vice President et al. on Human Treatment of al Qaeda and Taliban Detainees ¶ 2(d) (Feb. 7, 2002), *available at* http://www.washingtonpost.com/wp-srv/nation/documents/020702bush.pdf. While controversial, this category has a long historic pedigree. *See* John B. Bellinger III & Vijay M. Padmanabhan, *Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and other Existing Law*, 105 AMERICAN JOURNAL OF INTERNATIONAL 201, 217 n.80 (2011) (describing extensive support for the existence of this category).

62. Unlawful combatants are subject to detention based on their status as combatants until the end of hostilities. But they do not enjoy combatant immunity, meaning they are subject to prosecution in the civilian courts of the enemy State for actions taken during combat. They are also not entitled to prisoner of war privileges.

63. MELZER, *supra* note 21, at 27.

64. *Id.* at 34.

lar, operation-specific roles in the unit or general support roles.[65] Thus, a computer specialist whose role is limited to designing cyber weapons or collecting information about the nature of enemy infrastructure would be a civilian. By contrast, a similar specialist who modifies viruses to overcome the active defenses of the target, or who collects information about those defenses in order to operationalize an attack, would be considered a combatant.

Scholars have criticized this approach for being unduly restrictive in assigning combatant status to those in armed groups. Kenneth Watkin argues that it is artificial to divide integrated units that work together to accomplish a military objective into a mix of combatants and civilians. For example, he notes that crews that plant improvised explosive devices in Iraq and Afghanistan are units unto themselves, with different individuals within the unit responsible for weapons production, training, intelligence gathering and actual weapons launch. Watkin argues that to limit combatant status to triggermen is artificial, as the unit as a whole must be targetable in order to mitigate its threat.[66]

Watkin's criticism is somewhat less trenchant in the context of cyber weapons. The potentially complex nature of cyber weapons may require a blending of duties between those involved in attack preparation and launch, such that most members of a cyber unit would be sufficiently involved with a specific operation to be deemed combatants. Nevertheless, it is legitimate to question whether dividing members of a cyber unit based on function accurately reflects the cohesive, integrated threat such a unit poses to enemy infrastructure.

A different approach was tentatively explored by the D.C. District Court in the Guantanamo habeas cases. Two district court judges crafted a test that permitted the government to detain as enemy combatants those who receive and execute orders from the enemy's command structure because such individuals are within the "armed forces" of enemy non-State

65. Of course, hacktivists by definition have no "regular role" within any belligerent armed forces, and would thus be treated as civilians under this analysis. Similarly, those whose primary role is to guard civilian infrastructure but who get drawn into conflict while defending that infrastructure have no role in the belligerent armed forces and would be civilians, unless deemed part of a *levée en masse*.

66. *See* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 641, 680–82 (2010) (criticizing "continuous combat function" test as applied to irregular units).

organizations.[67] By contrast, those who merely supported the enemy through functions like propaganda or finance were not detainable as combatants.[68]

Such an approach applied to cyber warriors would allow entire cyber units, such as quasi-independent groups or contractors affiliated with a belligerent in an armed conflict, to be considered combatants if, in fact, the unit took orders and responded to orders from the belligerent. However, efforts by belligerents to mask their relationship with a cyber unit could make application of this test difficult. Targeting decisions will not be made with the benefit of the extensive process used in the detention context, where administrative or even court review is possible.

The key point is if cyber warriors can be categorized as unlawful combatants, then parameters for that category must be identified.

V. PROCESS

The fluid and imprecise nature of the categories described in Parts II–IV raise a difficult question: how will an actor deciding whether to use force obtain sufficient information to determine how to categorize a cyber warrior? Article 57(2) of Additional Protocol I mandates that those making targeting decisions "do everything feasible" to verify that the subject of the attack is not a civilian who is not directly participating in hostilities. International law recognizes that factors such as "time constraints, risks, technology, and resource costs" condition the obligation to obtain information to aid the targeting decision.[69] Thus, doing what is "feasible" to distinguish civilians requires exercising "reasonable care" in targeting decisions.[70]

---

67. Gherebi v. Obama, 609 F. Supp.2d 43, 68–70 (D.D.C. 2009); Hamlily v. Obama, 616 F. Supp.2d 63, 67–69 (D.D.C. 2009).

68. A panel of the U.S. Court of Appeals for the D.C. Circuit ultimately rejected the use of a detention standard based upon the IHL definition of "combatant." Al-Bihani v. Obama, 590 F.3d 866, 871 (2010). While the D.C. Circuit sitting *en banc* suggested this part of the opinion was dictum. Al-Bihani v. Obama, 619 F.3d 1, 1 (D.C. Cir. 2010) (Sentelle, J., concurring in denial of rehearing *en banc*), the Appeals Court has relied on *Al-Bihani* to reject the use of the command structure requirement as a limitation on the executive's detention authority. Awad v. Obama, 608 F.3d 1, 11–12 (D.C. Cir. 2010); Bensayah v. Obama, 610 F.3d 718, 725 (D.C. Cir. 2010).

69. *See* Matthew C. Waxman, *Detention as Targeting: Standards of Certainty and Detention of Suspected Terrorists*, 108 COLUMBIA LAW REVIEW 1365, 1389 (2008) (describing limits on State obligations in targeting decisions).

70. *See id.* at 1388 (marshaling evidence to support this standard).

Exercising reasonable care in the cyber context requires evaluating factors such as:[71]

- Affiliation between the cyber warrior and the belligerent;
- The function the cyber warrior serves within a cyber unit;
- Whether the cyber warrior's act "directly caused" the harm in question; and
- Whether the cyber warrior's participation in the hostilities continues.

These determinations are difficult because cyber warriors expend great effort to mask their identity. They also act in civilian environments far from any real battlefield, which raises the risk of misidentification.[72]

U.S. officials have yet to provide any guidance on what procedures the United States would employ before targeting an individual or property believed to be involved in a cyber attack on the United States. U.S. State Department Legal Adviser Harold Koh contends that this problem is a "technical and policy" challenge for States seeking to follow international law in responding to cyber attacks.[73] Development of procedural standards governing the targeting of cyber warriors is essential to reducing the legal uncertainties surrounding cyber operations.

Perhaps the closest analogy for targeting purposes is the procedures employed by the United States in its drone program targeting members of al Qaida in Yemen and Pakistan. While the exact nature of the inquiry conducted by U.S. officials to determine whether potential targets are lawful remains secret, Obama administration officials have indicated it involves

---

71. The process question is easier in the context of detention. One of the lessons emerging from the post-9/11 conflicts is that adversarial administrative and court procedures can be employed to reduce the risk of erroneous deprivations of liberty where there is serious risk of misidentification of alleged combatants. *See* Bellinger & Padmanabhan, *supra* note 61, at 221 (criticizing the decision of the Bush administration to provide minimal process to detainees in the conflict with al Qaida and the Taliban). The technical nature of cyber operations suggests that there may be the need for technical witnesses in determining whether a captured cyber warrior is a combatant or a civilian.

72. *See* Vijay M. Padmanabhan, *Legacy of 9/11: Continuing the Humanization of Humanitarian Law*, 14 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 419, 421–22 (2011) (describing a similar problem in the context of conflicts with non-State actors).

73. *See* Harold H. Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace, Remarks at the USCYBERCOM Inter-agency Legal Conference (Sept. 18, 2012) (describing challenges the United States faces in applying international law to cyber-conflicts).

assessment of intelligence information by a range of government officials, including the President himself.[74]

Targeting suspected cyber warriors will require a potentially more robust process, given the greater ease with which cyber fingerprints can be hidden and the technical nature of the attribution inquiry. But given that cyber operations can be part of more intense, ongoing armed conflicts than the U.S. conflict with al Qaida, such added process may not be realistic. For example, in the cataclysmic event of an armed conflict between the United States and China it would be unrealistic to expect high ranking government officials to spend time evaluating the decision to target individual cyber warriors.

VI. THE FUTURE

This article reveals the large number of difficult legal questions that arise when attempting to categorize cyber warriors for *jus in bello* purposes during an armed conflict. Some of these questions are particular to cyber; other questions reflect general lacunae in the law of armed conflict that have resonance in cyber operations. These questions include:

- When does a cyber warrior "belong to" a belligerent to the conflict?
- Must a cyber warrior affiliated with a State party distinguish himself visually in order to be categorized as a lawful combatant?
- Are all cyber warriors who are not lawful combatants civilians?
- If there is a category of unlawful combatants, what parameters define that category and how do those parameters apply to cyber warriors?
- How should the concept of direct participation in hostilities, including its temporal dimension, be applied to cyber warriors?
- What process should be implemented to resolve distinction questions in targeting?

---

74. *See* John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, The Ethics and Efficacy of the President's Counterterrorism Strategy, Remarks at the Woodrow Wilson International Center for Scholars (Apr. 30, 2012), *available at* http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy (providing bare bones account of targeting process); Jo Becker & Scott Shane, *Secret 'Kill' List Proves a Test of Obama's Principles and Will*, NEW YORK TIMES, May 29, 2012, at A1 (describing process in which Obama administration officials, including the President, debate the merits of killing potential targets in Yemen and Pakistan).

Given this multitude of questions, it is not surprising that scholars have begun to call for new international law to regulate cyberspace. Rex Hughes from the University of Cambridge has advocated for a multilateral treaty governing cyberspace.[75] Among the issues Hughes envisions such a treaty addressing is how to apply the principle of distinction to cyber warriors, including what, if any, modifications need to be made to rules distinguishing combatants from civilians.[76] In Hughes' favor is the current uncertain climate surrounding cyber capabilities. A world without clear understanding of relative cyber powers might be one that is willing to enter into an international agreement restricting and regulating its use. In this sense, we may in fact be, to steal a term from John Rawls, in a cyber "original position."

That said, there are at least two good reasons to be dubious about the prospects for a cyberspace treaty. First, as noted earlier, many of the questions that are contested in the area of cyber warriors are also contested in other areas of armed conflict. For example, conflicts with non-State actors like al Qaida have raised panoply of similar questions.[77] The fact that these questions are disputed in IHL writ large suggests that their resolution in a cyber treaty would be provocative and unlikely to attract international agreement.

Second, even at this early date there are significant disagreements about what regulation of cyberspace will look like. The British government has initiated an international forum to discuss regulation of cyberspace. That forum has already revealed deep disagreement about the areas of cyber most in need of regulation. Western States, including the United Kingdom and the United States, stress the need to protect computer networks and technological infrastructure from espionage and attack. China and Russia, by contrast, emphasize the need to regulate the dissemination of information across cyberspace, regulations that are anathema to the free speech human rights norm.[78] Failure to agree on the goals for regulation demonstrates how far apart the international community is on cyber regulation.

Instead there is a need for like-minded States actively grappling with cyber operations to think together about what form of future international

---

75. Hughes, *supra* note 19, at 524.

76. *See id.* at 537 (including distinction in issues for a future treaty).

77. *See generally* Bellinger & Padmanabhan, *supra* note 61 (describing areas of international law in need of further legal development to regulate conflicts with non-State actors).

78. *See* Nick Hopkins, *Britain in Talks on Cybersecurity Hotline with China and Russia*, GUARDIAN (Oct. 3, 2012), http://www.guardian.co.uk/politics/2012/oct/04/britain-cybersecurity-hotline-china-russia (describing areas of disagreement on cyber regulation).

regulation makes sense. Adam Segal and Matthew Waxman of the Council on Foreign Relations have argued that at this time the most that can be accomplished globally is for like-minded States to form partnerships on cybersecurity from which shared understandings on the use of force in response to cyber operations may emerge.[79] Including discussion of the legal problems created by cyber warriors will bolster the ability of IHL to remain relevant in regulating this rapidly changing area of warfighting.

79. *See* Adam Segal & Matthew Waxman, *Why a Cybersecurity Treaty is a Pipe Dream*, CNN WORLD (Oct. 27, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/.