ARTICLE

Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines

Brig. Gen. (ret.) David Wallace, Col. Shane Reeves, and Maj. Trent Powell*

* Brig. Gen. (Ret.) David Wallace is a Professor Emeritus, Department of Law, United States Military Academy at West Point, New York. Col. Shane Reeves is a Professor and Head, Department of Law, United States Military Academy at West Point, New York. Maj. Trent Powell is an Army judge advocate currently assigned as a LL.M. candidate at the University of Virginia Law School. The opinions, conclusions, and recommendations in this article do not necessarily reflect the views of the Department of Defense, the United States Army, or the United States Military Academy. The authors thank the editors of the Harvard National Security Journal for their assistance, including Sam Cohen, Philip Chertoff, Jon DeWitt, Mikhaila Fogel, Christopher Gorman, David Hogan, Annie Kapnick, Matthew Kahn, Anastasia Pyirinis, Sam Rebo, Diego Negron-Reichard, Kathryn Reed, and Avery Smith.

Abstract

Throughout history, civilians have contributed to nearly every armed conflict in a variety of roles that confer different protection under international law. They have supplied logistic, economic, administrative, and political support to belligerent parties. When such civilian contributions are indirect and away from battlefields, there is rarely much concern about those participating civilians jeopardizing their protected status under the Law of Armed Conflict (LOAC), which is one of the LOAC's central aims.

The civilian population and individual civilians enjoy general protections against dangers arising from military operations. Civilians are protected unless and for such a time as they take a direct part in hostilities. An act of direct participation in hostilities by civilians renders them liable to be attacked, and it subjects the participating civilians to prosecution and punishment to the extent that their activity, their membership, or the harm they caused is criminal under domestic law.

The notion of "taking a direct part in hostilities" is one of the most fundamental yet vexing concepts under the LOAC. Its application raises many challenging issues. For example, who precisely is considered a civilian under the LOAC? What conduct amounts to taking a direct part in hostilities? And, at what point does taking a direct part in hostilities begin and end? Understanding and applying the concept of direct participation in hostilities can be challenging. Belligerents increasingly use civilians in capacities that involve greater or more direct participation in hostilities. As complicated as these and related questions may seem, the concept of taking a direct part in hostilities presents even greater difficulties when applied in the context of cyber operations.

This Article provides a background and context on the dangerous trend towards increased civilian participation on modern battlefields and an overview of the legal concept direct participation in hostilities. It next considers Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0) rules and commentary as this resource pointedly addresses the notion of taking a direct part in hostilities in cyber operations. Finally, the Article concludes by outlining several important fault lines highlighted by the group of experts behind Tallinn Manual 2.0 in hopes of strengthening "the implementation of the principle of distinction" and, consequently, ensuring greater accountability in warfare.

Table of Contents

I. Introduction

Civilians contribute to nearly every war effort, and always have. Throughout history, non-military personnel have supplied logistic, economic, administrative, and political support to parties in armed conflicts. When civilian contributions are indirect and away from battlefields, there has historically been little concern about those participants jeopardizing their protected status under the Law of Armed Conflict (LOAC). More recently, however, belligerents have begun using civilians in capacities that involve greater or more direct participation in hostilities.[1] Some commentators have referred to this phenomenon as the "civilianization of armed conflict."[2]

Prior studies have identified at least four developments that contribute to civilians' growing participation in hostilities: (1) the privatization of warfare,[3] (2) a long-term shift toward non-international versus international armed conflicts, (3) the greater use of civilian proxies by States, and (4) the expanding role civilians play in high-technology warfare.[4] At the individual level, the consequences of civilians directly participating in hostilities are significant and several. Such civilians lose their immunity from attack during the period of time that they take a direct part in hostilities.[5] Additionally, civilians who directly participate in hostilities are subject to prosecution and punishment to the extent that their activities, their membership, or the harm they caused is criminal under domestic law.[6]

In the context of the LOAC, the protection of civilians is one of its underlying and primary goals. The civilian population and individual civilians enjoy general protections against dangers arising from military operations. In that regard, the LOAC explicitly provides that the civilian population, as well as individual civilians, shall not be the object of an attack and that civilians retain their

---

[1] *See, e.g.*, Shane R. Reeves & Ronald T.P. Alcala, *Five Legal Takeaways from the Syrian War*, HARV. NAT'L SEC. J. ONLINE, 3–4 (Sept. 30, 2019), https://harvardnsj.org/wp-content/uploads/sites/13/2020/04/Reeves-Alcala_Five-Legal-Takeaways-from-the-Syrian-War_FINAL.pdf [https://perma.cc/2DPL-GAEK] (last visited Nov. 14, 2020) (discussing the trend towards using private military contractors for offensive operations).

[2] *See, e.g.*, Andreas Wegner & Simon J.A. Mason, *The Civilianization of Armed Conflict: Trends and Implications*, 90 INT'L REV. RED CROSS 835, 836 (2008) (cataloguing factors that contribute to civilian-participants' changing role in hostilities).

[3] Most notably, recruiting and using private military and security companies to undertake certain traditional functions performed by members of armed forces illustrates this concept of "privatization of warfare."

[4] Wenger & Mason, *supra* note 2, at 835–52.

[5] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51(3), *adopted* June 8, 1977, 1125 U.N.T.S 3 [hereinafter AP I] ("Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.").

[6] INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (Nils Melzer ed., 2009), 83–85, *available at* https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf [https://perma.cc/63A5-FCBJ] (last visited Oct. 28, 2020) [hereinafter ICRC INTERPRETIVE GUIDANCE].

protections against attack unless and for such time as they take a direct part in an attack.[7] Critically important to the protection of civilians is the rule against taking direct part in hostilities.[8] In other words, the protections afforded individual civilians during an armed conflict is subject to an overriding condition, i.e., that they refrain from all hostile acts.[9] This principle is well grounded in both international treaties, including Additional Protocols I and II,[10] and through State practice where it has developed into a generally accepted norm of customary international law applicable to both international and non-international armed conflicts.[11]

Despite its seeming simplicity and straightforwardness, the notion of taking a direct part in hostilities—which is inextricably linked to the core LOAC principle of distinction—is one of the most vexing provisions under the LOAC.[12] Its application raises many challenging and thought-provoking issues. For example, who precisely is considered a civilian under the law of armed conflict? What conduct amounts to taking a direct versus indirect part in hostilities? What does "for such time" and "direct part" mean in practice? At what point does taking a direct part in hostilities begin and end?

In some instances, it is abundantly clear when a civilian is taking a direct part in hostilities. For instance, a civilian that engages an enemy soldier with a weapon during an international armed conflict is taking a direct part in hostilities and loses his or her protection under the LOAC.[13] Other circumstances are less obvious, including a situation where a civilian drives an ammunition vehicle during an armed conflict in support of a party to the conflict.[14] The LOAC supports the proposition that the vehicle is a targetable military objective, but a question remains whether the civilian driver is independently targetable for his or her actions. Did

---

[7] AP I, *supra* note 5, art. 51(2)–(3).
[8] *Id*. art. 51(3).
[9] *See* YVES SANDOZ ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JULY 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 1942–45 (1987) [hereinafter COMMENTARY].
[10] AP I, *supra* note 5, art. 51(3); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol II), art. 13(3), *adopted* June 8, 1977, 1125 U.N.T.S 609 [hereinafter AP II].
[11] Jean-Marie Henckaerts & Louise Doswald-Beck, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: VOLUME I: RULES, 19–24 (2005) [hereinafter RULES]. *But see* U.S. DEP'T OF DEF., LAW OF WAR MANUAL §5.9.1-.2, at 236–37 (2016) [hereinafter DOD LAW OF WAR MANUAL] (noting that the United States does not agree these rules as a matter of customary international law).
[12] GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 693 (2d ed. 2016).
[13] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, § 5.8.3.1 (listing examples where an individual is taking a direct part in hostilities). *See also* Stephen Pomper, *Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress Through PRactice*, 88 INT'L L. STUD. 181, 190 (2012) ("The period during which an individual can be deemed to be directly participating in hostilities is generally viewed to include the period during which that individual is deploying to and returning from the hostile act . . . .").
[14] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, § 5.8.3.2 (listing examples where an individual is not taking a direct part in hostilities).

the driver lose the LOAC protections during the period he or she was operating the vehicle?

As complicated as this question may seem, the notion of taking a direct part in hostilities presents even greater difficulties when applied to cyber operations. LOAC applies to cyber operations during armed conflicts,[15] and therefore, as Michael Schmitt notes, "[t]hose who qualify as combatants enjoy the belligerent right of engaging in hostilities; no reason exists to distinguish cyber from kinetic military operations in this regard."[16] Similar to kinetic situations, there are cyber actions that are obviously taking a direct part in hostilities and others that are not so clear. For example, if a civilian conducts a Distributed Denial of Service (DDoS) operation against an enemy's external computer systems during an armed conflict,[17] that civilian is taking a direct part in hostilities and becomes targetable while he or she is engaged in the DDoS attack.[18] By contrast, it is far less clear whether a civilian is taking a direct part in hostilities when he or she develops malware and provides it to others knowing that the malicious software will be used to attack an enemy at some unknown time.[19]

Determining when a civilian cyber operator in armed conflict is directly participating in hostilities is often even more challenging than the two examples provided above.[20] In most circumstances, the battlefield status of the individual remains unclear.[21] Yet, as cyber space has become a decisive battleground, it is important to provide clarity in how the LOAC applies in this domain[22] as legal

---

[15] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 375 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]. In 2017, states including Cuba and, reportedly Russia and China, backtracked on earlier recognition that the law of armed conflict applied in cyberspace. *See* Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SEC. (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [https://perma.cc/3QGA-AX2S]. However, the vast majority of the international community agrees that "international law applies to State-conducted or State-sponsored activities in cyberspace" and believe this is a settled question. *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, § 16.1; GARY P. CORN, "Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace," *in* LIEBER SERIES VOL. 1 COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE 399–400 (Ford & Williams 2019).

[16] Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INT'L L. STUD. 89, 97 (2011).

[17] TALLINN MANUAL 2.0, *supra* note 15, at 565 (A Distributed Denial of Service (DDoS) is a "technique that employs multiple computing devices (e.g., computers or smartphones), such as the bots of a 'botnet'…, to cause a 'denial of service'…to a single or multiple targets.").

[18] *Id.* at 430.

[19] *Id.*

[20] Schmitt, *supra* note 15, at 97.

[21] "On a battlefield no one is without some status." SOLIS, *supra* note 12, at 187. This "battlefield status" determines the associated rights, duties, and responsibilities of both warfare participants and other persons not engaged in the hostilities. *See* Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 392, 414–14 (2010).

[22] *See e.g.*, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA, 3 *available at* https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/4PJX-SYKF] (last visited Oct. 28, 2020) ("Today, every domain is contested—air, land, sea, space, and cyberspace.").

ambiguity "in no way relieves commanders or the lawyers advising them" of their obligations.[23] Therefore, this article attempts to address this issue by first providing a short background section on the dangerous trend towards increased civilian participation on modern battlefields. An overview of the legal concept "direct participation in hostilities" follows. The article then considers *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*)[24] rules and commentary as this resource pointedly addresses the notion of taking a direct part in hostilities in cyber operations. Finally, the article concludes by outlining several important fault lines highlighted by the group of experts behind *Tallinn Manual 2.0* in hopes of strengthening "the implementation of the principle of distinction"[25] and, consequently, ensuring greater accountability in warfare.

II. The Civilianization of Modern Warfare

The principle of distinction, at times characterized as fundamental or "intransgressible,"[26] requires the parties to an armed conflict to distinguish between civilians and combatants, directing attacks only against combatants and not against civilians.[27] Additionally, the parties must distinguish between civilian objects and military objectives.[28] The principle is universally recognized in both customary practice and treaty law as inviolable.[29] Yet, civilian participation in hostilities is both increasing and becoming more direct, undercutting the effectiveness of the foundational principle of distinction.

A. *Who Is a "Civilian" Under the Law of Armed Conflict?*

The commentary to Additional Protocol I to the 1949 Geneva Conventions notes that "protection of the civilian population is inseparable from the principle of distinction which should be made between military and civilian persons" and therefore "it is essential to have a clear definition of each of these categories."[30] Despite this exhortation, the term "civilian" is left undefined in the LOAC. Instead, Additional Protocol I, Article 50 describes a civilian in the negative as "any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol."[31]

---

[23] CORN, *supra* note 15, at 365.

[24] *See generally* TALLINN MANUAL 2.0, *supra* note 15.

[25] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 5.

[26] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8). The opinion goes on to state: "States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets." *Id.*

[27] RULES, *supra* note 11, at 3 (stating that attacks "may only be directed against combatants" and "must not be directed against civilians."). *See also* AP I, *supra* note 5, at art. 48; AP II, *supra* note 10, at art. 13(1) ("The civilian population and individual civilians shall enjoy general protections against the dangers arising from military operations.").

[28] RULES, *supra* note 11, at 25. *See also* AP I, *supra* note 5, art. 48; AP II, *supra* note 10, art. 13(1).

[29] Solis, *supra* note 12, at 251–57.

[30] COMMENTARY, *supra* note 9, ¶ 1911.

[31] AP I, *supra* note 5, art. 50. The article goes on to state "[i]n case of doubt whether a person is a civilian, that person shall be considered to be a civilian." *Id.* Those listed in Article 4(4) and (5),

Taken together, Articles 4A and 43 delineate and describe combatants that include: members of the armed forces of a party to the conflict, members of militias and organized resistance movements belonging to a party to the conflict, members of regular armed forces belonging to governments not recognized by the detaining power, and inhabitants of non-occupied territory who take up armed to fight an invading force.[32]

Based upon this broad definition, in international armed conflicts, individuals are therefore either combatants[33]—which also includes those who join a *levee en masse*[34]—or civilians.[35] If a combatant, the individual is targetable without any specific conduct unless they are considered a noncombatant member of the armed forces[36] or are *hor de combat*.[37] Further, a combatant is entitled to

---

which include journalists and others that may accompany the armed force, maintain their civilian status but are afforded prisoner-of-war status if captured. *See generally* Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III].

[32] Some States disagree with the Additional Protocol's definition of combatant and, consequently, its definition of a civilian. *See e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, §4.8.1.5 (defining a civilian as those who are "a member of the civilian population, *i.e.*, a person who is neither part of nor associated with an armed force or group, nor otherwise engaging in hostilities"); U.K. MINISTRY OF DEF., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT §5.3.1 (2004) [hereinafter U.K. MANUAL] (defining civilians as "persons who are not members of the armed forces").

[33] Combatants are defined generally as "[m]embers of the armed forces of a Party to a conflict," affording them "the right to participate directly in hostilities." *See* AP I, *supra* note 5, art. 43(2); INT'L & OPERATIONAL L. DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 16 (2012) ("Combatants are military personnel lawfully engaging in hostilities in an armed conflict on behalf of a party to the conflict …. [They] are also [a] *privileged* belligerent, i.e. authorized to use force against the enemy on behalf of the state."). For a comprehensive list of those considered combatants, see GC III, *supra* note 31, art. 4. Of note, AP I, article 44(3) allows a belligerent to attain combatant status by carrying his arms openly during each military engagement and when visible to an adversary while deploying for an attack. AP I, *supra* note 5, art. 44(3). "The Additional Protocol standard lowers the threshold for obtaining combatant status … by eliminating the classic requirement for 'having a fixed distinctive sign recognizable at a distance' . . . ." Derek Jinks, *Protective Parity and the Laws of War*, 79 NOTRE DAME L. REV. 1493, 1498 (2004). The U.S., concerned that the elimination of this requirement undercuts the principle of distinction, rejects Additional Protocol I, art. 44(3), as customary law and maintains the traditional combatant requirements outlined in the Geneva Conventions. *See* DOD LAW OF WAR MANUAL, *supra* note 11, §4.6.1.2.

[34] The concept of a *levee en masse* dates back to the French Revolution. *See* LAURIE R. BLANK & GREGORY P. NOONE, INTERNATIONAL LAW AND ARMED CONFLICT FUNDAMENTAL PRINCIPLES AND CONTEMPORARY CHALLENGES IN THE LAW OF WAR 214 (2013). A *levee en masse* occurs when the inhabitants of a non-occupied territory who, upon the approach of the enemy, spontaneously take up arms to resist the invading forces. *Id*. Given the urgency of the situation and the lack of time to prepare, such individuals do not have time to form themselves into regular armed units and therefore are considered combatants if they carry arms openly and respect the law of armed conflict. *Id*.

[35] *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 27 (2nd ed., 2010) (noting that the Law of Armed Conflict "posits a fundamental principle of distinction between combatants and civilians").

[36] Medical and religious personnel, though members of the armed forces, are considered noncombatants. SOLIS, *supra* note 12, at 191–94. *See also* INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 135–37 (2010).

[37] *See* LESLIE C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 124 (2nd ed. 2000) (stating

prisoner of war status if captured;[38] he or she is therefore immune from criminal prosecution under domestic law for activities, membership, or the harm that they may cause.[39] A civilian, on the other hand, is guaranteed "not only his life, health and dignity … but even his personal liberty."[40] However, this status is not absolute as a civilian only "enjoy[s] the protections afforded" by the Law of Armed Conflict "unless and for such time as they take a direct part in hostilities."[41] This bifurcated construct between combatants and civilians thus ensures any international armed conflicts are waged solely among the combatants of belligerent States with civilians only losing protected status should they actively participate in fighting.[42]

In non-international armed conflicts, battlefield status is significantly murkier as the law gives no guidance on what is meant by the term "civilian"[43] and combatant status does not apply.[44] That being said, the notion of "civilian" is clearly adopted in non-international armed conflicts.[45] This is partly evident through the provisions in Part IV of Additional Protocol II protecting individual civilians and the civilian population during non-international armed conflicts. Similarly, "parties to the conflict"—which include both the state's armed forces[46] as well as non-state

---

that combatants are lawful targets who are continuously a "legitimate object of attack, but only as long as they are capable of fighting, willing to fight or resist capture." *Hor de combat* is a French term that means "out of the battle." It is used as a term of art in LOAC to mean individuals who may not be attacked because they are out of the fight. For a comprehensive list of those considered "*hor de combat*" *see* AP I, *supra* note 5, art. 41.

[38] *See generally* GC III, *supra* note 31. *See also* DOD LAW OF WAR MANUAL, *supra* note 11, §4.3 (describing the rights and protections under the LOAC for a POW). A captured combatant is entitled to the status of prisoner of war "subject to the *conditio sine quo non*" that he is operating in accordance with the obligations required to attain combatant status. *See* DINSTEIN, *supra* note 35, at 29.

[39] DOD LAW OF WAR MANUAL, *supra* note 11, §4.4.3; Dieter Fleck, *The Law of Non-International Armed Conflict*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 613 (Dieter Fleck ed., 2d ed. 2008).

[40] DINSTEIN, *supra* note 35, at 29.

[41] AP I, *supra* note 5, art. 51(3); DINSTEIN, *supra* note 35, at 29–30 (noting that a civilian that takes up arms "or participate[s] actively in hostilities" forfeits the benefits of civilian status).

[42] DINSTEIN, *supra* note 35, at 27.

[43] *See* Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, 88 INT'L L. STUD. 119, 120 (2012) ("Unfortunately, Additional Protocol II, in contrast to its international armed conflict counterpart, offers no definition of the term 'civilian.'") (citation omitted).

[44] *See, e.g.*, U.K. MANUAL, *supra* note 32, §15.6.1 ("The law relating to internal armed conflict does not deal specifically with combatant status. . . ."). *See also* SOLIS, *supra* note 12, at 205 (stating that there are not combatants as understood in an international armed conflict in non-international armed conflicts).

[45] *See, e.g.*, AP II, *supra* note 10, art. 13 (discussing the general protections of the civilian population).

[46] *See generally* Sean Watts, *Present and Future Conceptions of the Status of Government Forces in Non-International Armed Conflict*, 88 INT'L L. STUD. 145 (2012) (discussing this particular battlefield status).

organized armed groups[47]—are also anticipated.[48] These are all mutually exclusive categories meaning that protections extended to civilians will not apply to those who belong to armed forces or organized armed groups.[49] Further complicating the distinction, civilians are only targetable "for such time as they take direct part in hostilities,"[50] whereas individuals who belong to the armed forces or an organized armed group are subject to attack even when not participating in hostilities.[51] Additionally, as there is no prisoner of war regime or concept of "combatant immunity" in a non-international armed conflict,[52] civilians who directly participate in the hostilities, or any members of an organized armed group, upon capture "may

---

[47] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.2.1 (citing Pomper, *Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress Through Practice*, *supra* note 13, at 193 n.22).

> The U.S. approach has generally been to refrain from classifying those belonging to non-State armed groups as "civilians" to whom this rule would apply. The U.S. approach has been to treat the status of belonging to a hostile, non-State armed group as a separate basis upon which a person is liable to attack, apart from whether he or she has taken a direct part in hostilities.

Id. For a detailed discussion on whether "organized armed groups other than the dissident armed forces comprise groups who are directly participating in hostilities or constitute a separate category of 'non-civilians,'" see also ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 28; SCHMITT, *supra* note 43, at 127.

[48] Clarification on who qualifies as a "Party to the conflict" in a NIAC is provided by Article 1(1) of the 1977 Additional Protocol II, which states:

> [t]his Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.

AP II, *supra* note 10, art. 1(1).

[49] *See* COMMENTARY, *supra* note 9, ¶4789 (discussing how individuals who belong to armed forces or armed groups are subject to attack at any time).

[50] AP II, *supra* note 10, art. 13(3).

[51] SCHMITT, *supra* note 43, at 127. *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.7.3 ("Like members of an enemy State's armed forces, individuals who are formally or functionally part of a non-State armed group that is engaged in hostilities may be made the object of attack because they likewise share in their group's hostile intent."); REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS 20 (Dec. 2016) [hereinafter U.S. USE OF MILITARY FORCE REPORT] (discussing the U.S. approach to targeting individuals in a NIAC).

[52] *See, e.g.*, U.K. MANUAL, *supra* note 32 §§15.6.1-2; DOD LAW OF WAR MANUAL, *supra* note 11, §17.4.1.1 (discussing how members of a non-State armed groups are not afforded combatant immunity).

be put on trial for treason or other crimes, and heavily punished."[53] The challenge, however, is determining when a civilian has forfeited their protections or, has gone further, and become a member of an organized armed group.[54]

B. *Cyber Space and the Problem of Civilian Participation in Warfare*

Whether as a victim or a participant, civilian involvement in armed conflicts is increasingly common on the contemporary battlefield.[55] This trend, sometimes called the "civilianization of armed conflict,"[56] is perhaps a foreseeable consequence of several macro-level operational developments including the private outsourcing of combat functions,[57] civilian proxy use by state parties,[58] and the proliferation of the technological advancements in the means and methods of war.[59] Regardless of the reason, this dangerous development undermines the LOAC's core principle of distinction,[60] and it dramatically increases risks for civilians during

---

[53] MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY, & YORAM DINSTEIN, The MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY 41 (International Institute of Humanitarian Law, 2006) (noting "[i]t should be understood, however, that trial and punishment must be based on due process of law."). Some states label these individuals "unprivileged belligerents" or "unlawful combatants." These terms do not connote a distinct individual battlefield status, *see* HCJ 769/02 Pub. Comm. Against Torture in Israel v. Gov't of Israel (2005) (Isr.), *at* http://elyon1.court.gov.il/files_eng/02/690/007/e16/02007690.e16.htm [https://perma.cc/6NZ7-Q9Y3] (last visited Nov. 14, 2020), but instead are descriptive for those who unlawfully engage in combat activities. *See* Knut Dormann, *The Legal Situation of "Unlawful/Unprivileged Combatants"*, 85 INT'L REV. RED CROSS 45 (2003), *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5LPHBV/ [https://perma.cc/3YDS-QDTG] (last visited Nov. 14, 2020). For a discussion on the adverse consequences of the being titled a "unprivileged belligerent" see Shane R. Reeves & David Lai, *A Broad Overview of the Law of Armed Conflict in the Age of Terror, in* THE FUNDAMENTALS OF COUNTERTERRORISM LAW 139, 146–47 (Lynne Zusman ed., 2014).

[54] *See generally* E. Corrie Westbrook Mack & Shane R. Reeves, *Tethering the Law of Armed Conflict to Operational Practice: "Organized Armed Group" Membership in the Age of ISIS,* 36 BERKELEY J. INT'L L. 355–382 (2018) (discussing and comparing the various approaches to determining membership in an organized armed group); MARCO SASSÒLI ET AL., HOW DOES LAW PROTECT IN WAR 263 (2011).

[55] *See* Wenger & Mason, *supra* note 4, at 835 (discussing the increasingly important roles civilians play in armed conflict as both victims and perpetrators).

[56] *See* Wegner & Mason, *supra* note 2.

[57] *See generally* Laura A. Dickinson, *Military Lawyers, Private Contractors, and the Problem of International Law Compliance*, 42 N.Y.U. J. INT'L L. & POL'Y 355–88 (2010) (discussing the use of private contractors for military functions).

[58] *See, e.g.,* Allison Quinn, *Vladimir Putin Sent Russian Mercenaries to 'Fight in Syria and Ukraine,'* TELEGRAPH (Mar. 30, 2016), https://www.telegraph.co.uk/news/2016/03/30/vladimir-putin-sent-russian-mercenaries-to-fight-insyria-and-uk/ [perma.cc/983X-6HSW] (last visited DATE).

[59] *See generally* MATTHEW T. KING, "High-Tech Civilians, Participation in Hostilities, and Criminal Liability," *in* LIEBER SERIES VOL. 2 THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT 175, 176 (Eric T. Jensen & Ronald T.P. Alcala eds., 2019) (noting "the blurring, flattening, and expanding of the battlefield brought about by new technologies.").

[60] AP I, *supra* note 5, art. 48 ("In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives. . . .").

armed conflict. It is, then, not surprising that civilians are killed and injured at much higher rates than their combatant counterparts in modern armed conflict.[61]

Perhaps nowhere is the civilianization of warfare issue more acute than in cyber operations, where civilians act as proxies, as unaffiliated but supportive "patriotic hackers," and as direct supplements to states' armed forces. Russia's aggression in Ukraine—where it has relied heavily on civilian hackers to serve as its proxies in carrying out hostile cyber operations[62] against critical infrastructure, political systems, and other important targets[63]—highlights the severity of the problem. However, Russia is by no means alone in the practice as States have long followed the political incentive to use proxies in kinetic warfare as in cyber to preserve "plausible deniability."[64] Analogizing the use of civilian cyber proxies to the maritime practice of states using privateers beginning in the seventeenth century, one scholar notes how "[i]f a 'private' undertaking that a ruler authorized met with success, s/he could claim a share in the profits. If the enterprise caused conflict with another state, the ruler could claim it was a private operation for which s/he could not be held responsible."[65] Likewise, cyber proxies act as non-

---

[61] *See, e.g.*, Adam Roberts, *Lives and Statistics: Are 90% of War Victims Civilians?*, 52 SURVIVAL 115, 118 (2010); Neta C. Crawford, *Human Cost of the Post-9/11 Wars: Lethality and the Need for Transparency*, COSTS OF WAR (Nov. 2018), https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Human%20Costs%2C%20Nov%208%202018%20CoW.pdf [https://perma.cc/S6WV-Q6BY] (last visited June 8, 2020); Mujib Mashal, *Afghan and U.S. Forces Blamed for Killing More Civilians This Year Than Taliban Have*, N.Y. TIMES (July 30, 2019), https://www.nytimes.com/2019/07/30/world/asia/afghanistan-civilian-casualties.html [https://perma.cc/V4V9-TVTL] (last visited Jun. 8, 2020); Murtaza Hussain, *It's Time for America to Reckon with the Staggering Death Toll of the Post-9/11 Wars*, INTERCEPT (Nov. 19, 2018), https://theintercept.com/2018/11/19/civilian-casualties-us-war-on-terror/ [https://perma.cc/34HW-F784] (last visited June 8, 2020).

[62] *See* Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA ANALYSIS & SOLUTIONS 19-22 (Mar. 24, 2017), https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf [https://perma.cc/BR9Q-EHAD] (last visited June 8, 2020); Andrew Kramer, *How Russian Recruited Elite Hackers for Its Cyberwar*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html [https://perma.cc/EN49-F5LV] (last visited June 8, 2020).

[63] *See, e.g.*, Lauren Cerulus, *How Ukraine became a test bed for cyberweaponry*, POLITICO (Feb. 20, 2019), https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ [https://perma.cc/79ME-KWQN] (last visited June 8, 2020); *see also* Zak Doffman, *Russia Unleashes New Weapons In Its 'Cyber Attack Testing Ground': Report*, FORBES (Feb. 5, 2020), https://www.forbes.com/sites/zakdoffman/2020/02/05/russia-unleashes-new-weapons-in-its-cyber-attack-testing-ground-report/#44beee6c5ce5 [https://perma.cc/3QTN-HEKB] (last visited June 8, 2020).

[64] *See, e.g.*, Jordan Brunner, *Iran Has Built an Army of Cyber-Proxies*, Aug. 2015, TOWER, http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/ [https://perma.cc/CYK5-MMWX] (last visited Nov. 8, 2020). *See also* Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," *in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE 79, 81 (Kenneth Geers ed., 2015), https://www.ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf [https://perma.cc/WQ3M-FDG8] (last visited Nov. 15, 2020).

[65] *See* Maurer, *supra* note 64, at 81.

attributable intermediaries whose use comes with minimal political or legal consequences.

Similarly, so called "patriotic hackers" are a problematic group of civilians. These actors conduct cyber operations based upon independent loyalty or fealty to a state allowing that state the ability to project power while obfuscating legal responsibility.[66] Although outside the context of an armed conflict, a pertinent example of patriotic hacking occurred in Estonia in 2007.[67] Following the highly controversial relocation of the Bronze Soldier, a Soviet war memorial, from the center of Tallinn to a military cemetery, Estonian websites of government ministries, political parties, newspapers, banks, and companies became targets of DDoS operations in protest of the relocation.[68] Evidence indicated the operations originated from Russian IP addresses[69] and were conducted by a small group of Russian activists associated with the pro-Kremlin youth group, Nashi.[70] Despite repeated requests from the Estonian government, Russia refused to help or acknowledge responsibility for the Nashi's actions.[71]

Further, civilians are not only used by states on the periphery of cyber warfare, but with the technical complexity of modern weapons growing, they are progressively becoming important as direct supplements to armed forces.[72] In fact, civilians are now often doing mission-critical support functions in many military high-tech engagements.[73] Whether administering army battle command systems, managing communications systems, or helping employ sophisticated weaponry, civilian personnel are clearly an essential component of modern armed forces. [74]

What becomes apparent is that civilians—either as proxies or in direct support of a state's armed forces—are increasingly active in conflicts.[75] But "closer civilian involvement in the battlefield, either in a geographic sense or a function, causal [manner],"[76] is clearly making individual classification determinations difficult. The civilianization of warfare creates particular challenges when it comes to characterizing the legal status of the high-tech civilians prominent in cyber warfare.[77] Yet, determining that status is the critical first step in ensuring compliance with the principle of distinction and requires understanding what

---

[66] *See, e.g.*, Christian Lowe, *Kremlin Loyalist Says Launched Estonia Cyber-attack*, REUTERS (Mar. 13, 2009), https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 [https://perma.cc/9BJM-HCSK] (last visited Oct. 20, 2020).
[67] *Id*.
[68] *Id*.
[69] *Id*.
[70] *Id*.
[71] *See* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), http://www.bbc.com/news/39655415 [https://perma.cc/V9L4-GTCT] (last visited Oct. 28, 2020).
[72] *See* Wenger & Mason, *supra* note 2, at 839.
[73] *See id*.
[74] *See id*.
[75] *See* KING, *supra* note 59 at 175–77.
[76] *Id.* at 176.
[77] *Id.* at 176.

constitutes "direct participation in hostilities." The next section discusses the concept.

III. Direct Participation in Hostilities: An Overview

Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II contain the legal provisions concerning "direct participation in hostilities." Each of these articles generally states that "civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities."[78] A vast majority of states find that these rules reflect customary law in both international and non-international armed conflicts.[79] Even those states that disagree, such as the United States,[80] support the underlying customary principle. Accordingly, there is general agreement that the phrase "direct participation in hostilities" describes "when civilians forfeit their protection from being made the object of attack."[81]

However, despite the common usage of the phrase "direct participation in hostilities," views diverge on how this legal standard applies. This section explores some of the competing interpretations on the application of this standard. Subpart A discusses the efforts of the International Committee of the Red Cross (ICRC) to distill an analysis of "direct participation in hostilities" into a workable framework, while also illustrating some of the shortcomings. Subpart B further examines the ICRC project, offering views of influential states and a less rigid approach to a "direct participation in hostilities" analysis. Finally, Subpart C highlights the challenges in applying the ICRC legal standard to cyber space operations.

A. *ICRC's Interpretive Guidance*

In hopes of providing a uniform understanding, the ICRC launched a comprehensive research effort to explore the notion of direct participation by civilians in hostilities. In May 2009, the ICRC published the culmination of this

---

[78] AP I, *supra* note 5, art. 51(3); AP II, *supra* note 10, art. 13(3). The two provisions are identical except that Additional Protocol uses the term "section" in where Additional Protocol II says "part."

[79] *See* RULES, *supra* note 11, at 19-21.

[80] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.1.2 (*citing* John B. Bellinger, *Unlawful Enemy Combatants,* DIG. U. S. PRAC. INT'L L., Jan. 2007, at 915–16 ("Although, as drafted, Article 51(3) of AP I does not reflect customary international law, the United States supports the customary principle on which Article 51(3) is based."). While the United States has not ratified Additional Protocol I or II, many portions of the protocols are considered customary international law, including the protection of civilians during conflict and the principle of distinction. *See generally* Michael J. Matheson, *Remarks on the United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions,* 2 AM. U.J. INT'L L. & POL'Y 419 (1987).

[81] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.1.1 (noting that Common Article 3 "refers to [p]ersons taking no active part in the hostilities" while AP I and II use the phrase "direct participation in hostilities" and how distinguishing between these terms is of no value when applying the legal rule) .

process as the *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*.[82]

To appreciate the *Interpretive Guidance*, it is important to first understand that the ICRC is an exclusively humanitarian organization with a mission "to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance."[83] Working from that perspective, and in support of these laudable aims, the ICRC launched the project to provide recommendations on how direct participation in hostilities should be interpreted under existing law.[84] In doing so, the *Interpretive Guidance* describes three elements of direct participation in hostilities.[85]

i. The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm), and

ii. there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation), and

---

[82] *See generally* ICRC INTERPRETIVE GUIDANCE, *supra* note 6; *see also*, Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT'L SEC. J. 5, 5 (2010). The ICRC Interpretive Guidance research effort was undertaken in cooperation with the T.M.C. Asser Institute.

[83] INT'L COMM. RED CROSS, *The ICRC's Mandate and Mission*, https://www.icrc.org/en/mandate-and-mission [https://perma.cc/AK7N-93XH] (last visited Feb. 22, 2019). The legal basis of actions by the ICRC in an international armed conflict is rooted in the 1949 Geneva Conventions and Additional Protocol I. *Id.* In a non-international armed conflict, its legal mandate is in Common Article 3. *Id.* That is, the ICRC has a right of humanitarian initiative under those circumstances. *Id.* Finally, during internal disturbances and tensions, and in other circumstances that warrant humanitarian action, the ICRC likewise enjoys a right of initiative. *Id.* This right of initiative is in the Statutes of the International Red Cross and Red Crescent Movement. *Id.*

[84] The final report draws on multiple sources including the rules and principles of customary and treaty law, military manuals, other sources of relevant international law, and where necessary and appropriate, the *travaux préparatoires* of treaties. In French, *travaux préparatoires* means "preparatory ." *Travaux Préparatoires*, BLACK'S LAW DICTIONARY (11th ed. 2019). It is comprised of the "[m]aterials used in preparing the ultimate form of an agreement or statute." *Id.* As such, it constitutes legislative history. *See id.* Article 32 of the Vienna Convention on the Law of Treaties specifies that the preparatory work of the treaty and the circumstances of its conclusion may be used as a supplementary means of treaty interpretation. Vienna Convention on the Law of Treaties of 23 May 1969, art. 32, Jan. 27, 1980, 1155 U.N.T.S. 331, 8 I.L.M. 679. *See* INT'L COMM. RED CROSS, *Overview of The ICRC's Expert Process (2003–2008)*, https://www.icrc.org/eng/assets/files/other/overview-of-the-icrcs-expert-process-icrc.pdf [https://perma.cc/6A8W-9ZEK] (last visited Nov. 15, 2020) (noting that the report does not seek to change the existing LOAC)].

[85] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 6, 13.

iii. the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).[86]

We address each in order.

1. Threshold of Harm

The first element is commonly referred to as the "threshold of harm."[87] It is satisfied when a civilian act is reasonably anticipated to cause harm of a military nature regardless of its gravity.[88] The array of qualifying harm is not limited to the infliction of death, injury, or destruction of military personal or objectives. Rather, it is more broadly construed to include any consequences adversely impacting the military operations or capacity of the targeted party.[89] Accordingly, acts of sabotage and other activities, whether armed or unarmed, can meet the threshold of harm by restricting, impeding, or otherwise limiting logistical support, movement, and communications of the targeted enemy.[90] This criteria is also not limited to physical harm.[91] Interference with military computer networks or communications, for example, may suffice if the interference is likely to adversely affect military operations or capacity.

2. Direct Causation

The second element, "direct causation," requires a causal link between the civilian's action and the subsequent harm.[92] The commentators to the *Interpretive Guidance* described the directness between the act and harm as occurring in one causal step.[93] This element considers that the harm results from either the act itself, or from a military operation of which the act constitutes an integral part.[94] Examples of civilian acts that meet these criteria include attacking members of an opposing armed force, attempting to capture enemy weapons or equipment, laying mines, and detonating bombs.[95] These acts of direct participation would divest individuals of their immunity from attack under the LOAC. By contrast, indirect participation does not. Indirect participation involves activities in general support of the war effort and otherwise war-sustaining activities.[96] A paradigmatic example of indirect participation is civilians working in a factory that is not in geographic or temporal

---

[86] *Id.*, at 46.
[87] *See* SOLIS, *supra* note 12, at 218 (stating physical harm is not necessary to satisfy this criteria. Rather, there must simply be an objective likelihood that a harm would result).
[88] *Id.* at 47.
[89] *Id.* at 47-8.
[90] *Id.* at 48.
[91] *See* MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 204 (2014).
[92] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 51.
[93] *See id.* at 53.
[94] *Id.* at 53.
[95] A.P.V. ROGERS, LAW ON THE BATTLEFIELD 11 (2007).
[96] *See See* DOD LAW OF WAR MANUAL, *supra* note 11, *§5.8.3.2*.

proximity to military operations but that is providing weapons, materiel, and other goods useful to a party to an armed conflict.[97]

Germane to this Article is the distinction the *Interpretive Guidance* draws between *causal* proximity and *temporal* or *geographic* proximity. For example, many weapons or munitions operate with a time–delayed or remote trigger, including mines, booby-traps, or, in the cyber domain, malware. Malware can be inserted into an adversary's computer system to activate and perform its malicious function at some point in the future or upon the conclusion of precedent condition(s).[98] Similarly, modern warfare is replete with examples of geographic remoteness, including unmanned aerial vehicles, long-range missile systems, and cyber weapons. Neither geographic nor temporal distance between the civilian's action and the harm it breaks the causal link under the *Interpretive Guidance* framework.[99]

3. Belligerent Nexus

The third element, "belligerent nexus," requires the civilian's act to be specifically designed to directly cause the required threshold of harm *in support of one party to the conflict* and *to the detriment of another*.[100] Suppose a civilian robs a private bank during a period of armed conflict. While escaping, the civilian exchanges gunfire with government agents. The civilian's criminal act of violence is independent of the armed conflict; it is simply happening at the same time and place. Under this set of facts, there is no belligerent nexus because the civilian bank robber is not intended to harm the government in support of another belligerent.[101] A typical example of an action that lacks a belligerent nexus is an act of self-defense or an act in defense of others. Suppose a civilian is defending herself from an unlawful attack by an enemy soldier during an international armed conflict. The civilian's actions to defend herself cannot be regarded as taking a direct part in hostilities with its corresponding loss of immunity.[102]

B. *When Does Direct Participation Begin and End?*

Taken together, the three elements provide an analytical framework to determine whether a civilian's conduct qualifies as "taking a direct part in hostilities," thereby jeopardizing his or her protected status under the LOAC for the period of participation. However, the *Interpretive Guidance* attempts to answer a

---

[97] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 53 (stating that while these activities most assuredly result in harm to an enemy, they are considered insufficiently direct to meet this element). *But see* Reeves & Alcala, *supra* note 1, at 1–2 (discussing the difference between "war sustaining" and "war supporting" objects in regard to the United States approach to the law of targeting). *See also See* DOD LAW OF WAR MANUAL, *supra* note 11, *§5.8.3.2*.

[98] TALLINN MANUAL 2.0, *supra* note 15, at 566. This type of malware is often referred to as a "logic bomb."

[99] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 55.

[100] *Id.* at 58.

[101] SOLIS, *supra* note 12, at 219.

[102] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 61.

closely related question: when "direct participation" begins and ends. In other words, what are the legal and practical boundaries of "for such time" under Article 51(3)?[103] Underpinning this issue is the "revolving door" problem, in which a civilian repeatedly forfeits and then regains immunity by directly participating in hostilities, then ceasing the conduct, and then participating again.[104] Some refer to the revolving door scenario as "farmer by day, guerilla by night."[105] This course of conduct provides the farmer-guerilla a decided advantage over lawful combatants. While lawful combatants may be attacked at any time, the farmer-guerilla gains protection from attack any time he ceases directly participating in hostilities.[106] Therefore, to mitigate this advantage, it becomes important to precisely describe when "direct participation in hostilities" begins and ends.

Unquestionably, according to the *Interpretive Guidance*, the start of direct participation includes the execution phase of a qualifying act.[107] But what preparatory measures amount to direct participation? The *Interpretive Guidance* comments as follows: "[w]hether a preparatory measure amounts to direct participation in hostilities depends on a multitude of situational factors that cannot be comprehensively described in abstract terms."[108] These factors may include, but are not limited to, the military nature of the preparatory acts as well as the nexus to the subsequent execution of a specific hostile act.[109] Further, preparatory measures aimed at carrying out a specific hostile act qualify as direct participation.[110] For example, the loading of bombs on an aircraft for an attack against the enemy is direct participation even if the attack is the following day. By contrast, preparatory measures aimed at establishing the general capacity to carry out unspecified hostile acts do not qualify. A civilian does not directly participate in hostilities by transporting munitions for storage at an airfield for some unspecified future attack.[111] The essence of the distinction lies in differentiating between acts preparatory to combat and acts intended to create a general capacity to wage war.[112] In sum, the specific or general nature of the preparatory action is determinative of whether preparation amounts to direct participation.

When determining the ending of direct participation, the *Interpretive Guidance* emphasizes an understanding of the terms "deployment" and "return."[113] In some cases of direct participation, the civilian(s) must geographically deploy to commit the act in question.[114] Such deployments amount to an integral part of the participatory act. Similarly, if the return from the execution of an act is still an

---

[103] AP I, *supra* note 5, at art. 51(3); AP II, *supra* note 10, art. 13(3).
[104] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.4.2.
[105] *See id.*
[106] *See id.*
[107] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 53.
[108] *Id.* at 65.
[109] *Id.* at 65–66.
[110] *Id.*
[111] *Id.* at 66.
[112] *See* WILLIAM H. BOOTHBY, THE LAW OF TARGETING 159 (2012).
[113] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 67.
[114] *See id.*

integral part of the operation, it is effectively a military withdrawal. The return is finished once the person has physically separated from the operation. Evidence of the ending of participation includes stowing away or hiding weapons and munitions and other equipment used for the operation.[115] Civilians participating in these operations lose their immunity from the time the physical deployment begins until the return is finished. Where no geographic deployment is necessary, such as with cyberattacks, civilian participation includes only "immediate execution of the act and preparatory measures forming an integral part of that act."[116]

C. *The Interpretive Guidance's Unfortunate Legacy: Controversy*

The *Interpretive Guidance* addresses several tangential topics related to direct participation in hostilities and,[117] undoubtedly, advances the general understanding of the topic.[118] However, while the "planned output of the project was a consensus document," in fact "the proceedings proved highly contentious" with the disagreements varying by nature and degree.[119] As a result, several outside experts[120] withdrew from the project "lest inclusion be misinterpreted as support for the Interpretive Guidance's propositions."[121] This led the ICRC to take the "unusual step of publishing the Interpretive Guidance without identifying participants."[122] As a result, the report contained the "express caveat that it is 'an

---

[115] *See id.*

[116] *See id.* at 68.

[117] For example, the *Interpretive Guidance* developed the term "continuous combat function" (CCF) to differentiate between integrated members of an organized armed group (OAG) and civilians who take a direct part in hostilities on an infrequent or unorganized basis. *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 27. In outlining the parameters of the CCF concept, the *Interpretive Guidance* states: "[c]ontinuous combat function requires lasting integration into an organized armed group acting as the armed forces of a non-State party to an armed conflict." *Id.* at 34. The consequences of being a member of an OAG are severe ,as the individual is no longer targetable based upon their conduct but, rather, based on their status. *See id.* at 22 (explaining why individual members of an OAG should not be considered civilians); Schmitt, *supra* note 43, at 137 ("there is no LOAC prohibition on attacking members of organized armed groups at any time. . . ."). While outside the scope of this Article, the *Interpretive Guidance*'s CCF approach has also triggered a strong counter-response by both states, *see, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, §5.7.3 ("individuals who are formally or functionally part of a non-State armed group" are subject to attack), and scholars, *see, e.g.*, Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641, 691–92 (2010) ("Someone who provides logistics support as a member of an organized armed group, including cooks and administrative personnel, can be targeted in the same manner as if that person was a member of regular State armed forces."). For a detailed analysis of the various approaches to determining membership in an OAG, *see generally* Mack & Reeves, *supra* note 54, at 355–82.

[118] *See* Schmitt, *supra* note 82, at 6.

[119] *Id. See generally* ICRC INTERPRETIVE GUIDANCE, *supra* note 6.

[120] The *Interpretive Guidance* brought together 40–50 legal experts drawn from the armed forces, government, NGOs, and academia, all participating in their personal capacity. *See* INT'L COMM. RED CROSS, *Overview of The ICRC's Expert Process (2003-2008)*, https://www.icrc.org/eng/assets/files/other/overview-of-the-icrcs-expert-process-icrc.pdf [https://perma.cc/W4MP-MYHM] (last visited Feb. 22, 2019).

[121] *See* Schmitt, *supra* note 82, at 6.

[122] *Id.*

expression solely of the ICRC's views.'"[123]

The controversy surrounding the *Interpretive Guidance* has limited the document's influence with certain state actors. For example, the United States "made clear that it did not regard the study as an authoritative statement of law,"[124] expressly rejecting significant parts of the *Interpretive Guidance* as reflecting customary international law.[125] This is an unfortunate result, as it only states that can "reject, revise, or supplement" the LOAC or "craft new norms;" the ICRC may only promulgate proposals for states to consider.[126] It is therefore worth highlighting the general underlying criticism to the *Interpretive Guidance* as well as offering an alternate, state-centric interpretation of "direct participation in hostilities."

D. *A "Less Rigid" Approach to Direct Participation in Hostilities*

While specific criticisms of the *Interpretive Guidance* vary—including, for example, how the report defines the term "civilian" and interprets the "for such time as" treaty language[127] —underlying all concerns is a perception that the document unduly favors considerations of humanity over military necessity.[128] This overarching criticism illustrates a significant dilemma because, at its core, the LOAC is "predicated on a subtle equilibrium between two diametrically opposed impulses: military necessity and humanitarian considerations."[129] The balance between these competing principles is delicate,[130] and an over-emphasis on either

---

[123] *Id.* (*citing* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 6).

[124] Pomper, *supra* note 13, at 186.

[125] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.1.2 (*citing* Al-Bihani v. Obama, 590 F.3d 866, 885 (D.C. Cir. 2010) (Williams, J., concurring) ("The work itself explicitly disclaims that it should be read to have the force of law. . . . Even to the extent that Al Bihani's reading of the Guidance is correct, then the best he can do is suggest that we should follow it on the basis of its persuasive force.").

[126] Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VA. J. INT'L L. 795, 799 (2010).

[127] Many of the experts who withdrew from the project were from states specially affected by the *Interpretive Guidance*—such as the United States, the United Kingdom, and Canada—and they captured their disagreements in a series of articles. *See, e.g.,* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641–93 (2010); Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements,* 42 N.Y.U. J. INT'L L. & POL'Y 697 (2010); William H. Boothby, *"And For Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL'Y 741 (2010); W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect,* 42 N.Y.U. J. INT'L L. & POL'Y 770 (2010).

[128] Schmitt, *supra* note 82, at 6.

[129] YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW INTERNATIONAL ARMED CONFLICT 17 (1st ed. 2004) . *See generally* Schmitt, *supra* note 128; David A. Wallace & Shane R. Reeves, *Protecting Critical Infrastructure in Cyber Warfare: Is it Time for States to Reassert Themselves?,* 53 U.C. DAVIS L. REV. 1618 (2020) ("[T]hese two broad, often times called 'meta' principles are weighed against each other throughout the entirety of the law of armed conflict with every rule or norm—whether treaty or custom-based—considering both military necessity and the dictates of humanitarian aims.").

[130] *See* Brian J. Bill, *The Rendulic "Rule": Military Necessity, Commander's Knowledge, and*

upsets the "dialectical relationship [that] undergirds virtually all rules" of the LOAC.[131] The impression that the *Interpretive Guidance* favors humanitarian concerns is therefore dangerous and challenges the LOAC's effective regulation of warfare.[132] More specifically, the report is potentially viewed as creating unrealistic restrictions on military actions,[133] which is problematic as no state "likely to find itself on the battlefield would accept norms that place its military success, or its survival, at serious risk."[134]

For example, the *Interpretive Guidance*'s constitutive elements are generally accepted as reflecting the appropriate factors to be considered when analyzing a civilian's actions on the battlefield.[135] However, rigid application of the elements is strongly opposed by those states actively engaged in military operations. These states instead argue that "[a]ny determination that a civilian is taking part in hostilities (and thus loses immunity from being made the object of attack) [is] highly situational"[136] and based on "totality of the circumstances."[137] Thus, not all three constitutive elements need to be present to determine that a civilian is directly participating in hostilities. Adopting this case-by-case approach, the United Kingdom notes that "[w]hether civilians are taking a direct part in hostilities is a question of fact" and provides a few illustrative vignettes.[138] The

---

Methods of Warfare, 2009 Y.B. INT'L HUMANITARIAN L. 119, 128 ("Human life is no less valuable in war than in peace, but the need to resolve the contention between states through recourse to armed conflict has been permitted to outweigh that value in certain circumstances. In other circumstances . . . the balance remains tipped towards humanitarian concerns.").

[131] Schmitt, *supra* note 82, at 6.

[132] *See* DINSTEIN, *supra* note 129, at 1("Some people, no doubt animated by the noblest humanitarian impulses, would like to see zero-casualty warfare. However, this is an impossible dream. War is not a chess game. Almost by definition, it entails human losses, suffering and pain. As long as it is waged, humanitarian considerations cannot be the sole legal arbiters of the conduct of hostilities.").

[133] Shane R. Reeves & Jeffrey S. Thurnher, *Are We Reaching a Tipping Point? How Contemporary Challenges Are Affecting the Military Necessity-Humanity Balance*, HARV. NAT'L SEC. J. ONLINE (2013), http://harvardnsj.org/2013/06/are-we-reaching-a-tipping-point-how-contemporary-challenges-are-affecting-the-military-necessity-humanity-balance [https://perma.cc/CG27-CSJM] (last visited Dec. 29, 2019) ("when humanitarian concerns become dominant state military actions are unrealistically restricted by burdensome regulations diminishing the likelihood of compliance.").

[134] Schmitt, *supra* note 82, at 6.

[135] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.3 (laying out similar considerations relevant to a direct participation in hostilities analysis); U.K. MANUAL, *supra* note 32, §5.3.3. *See also* Schmitt, *supra* note 126, at 738 ("Of the three major foci of the notion of direct participation, the constitutive elements of direct participation set forth in the Interpretive Guidance prove the most satisfactory."); Pomper, *supra* note 13, at 190 (noting that nature of harm, causation, and nexus to hostilities are the general considerations taken into account by any decision-maker making a direct participation in hostilities analysis).

[136] Pomper, *supra* note 13, at 190.

[137] *Id. See also* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.3 (*citing* Pomper, *supra* note 13, at 189–90).

[138] U.K. MANUAL, *supra* note 32, §5.3.3. Specifically, the manual notes: "Civilians manning an anti-aircraft gun or engaging in sabotage of military installations are doing so. Civilians working in military vehicle maintenance depots or munitions factories or driving military transport vehicles are not, but they are at risk from attacks on those objectives since military objectives may be attacked whether or not civilians are present." *Id.*

United States, for its part, states that "[w]hether an act by a civilian constitutes taking a direct part in hostilities is likely to depend highly on context, such as the weapon systems or methods of warfare employed by the civilian's side in the conflict."[139] It then goes on to give a non-exhaustive list of behaviors that would or would not qualify as directly participating in hostilities.[140]

Similarly, these states take a more practical approach to determining the duration of a civilian's participation in hostilities. While acknowledging a spectrum of views on the topic,[141] they categorically deny any interpretation that provides "revolving door" protection for a civilian.[142] States take this position for several reasons. First, the "farmer by day and a guerilla by night" dynamic creates a legal inequity as the civilian using the "revolving door" gains protection from attack while a lawful combatant is targetable at any time based upon their status.[143] Second, the "revolving door" puts the civilian population in greater danger by blurring the line between a civilian who has forfeited protection and one that has not.[144] Third, providing off-and-on protections encourages abuse of the law thus incentivizing bad behavior. As a result, states with an operational perspective often reject the *Interpretive Guidance's* temporal scope analysis and take a simpler approach to duration determinations. The United States, for example, states that "civilians who have taken a direct part in hostilities must not be made the object of attack after they have *permanently* ceased their participation," (emphasis added) and, in those difficult situations where it is unclear, "a case-by-case analysis of the specific facts would be needed."[145]

E. *Addressing the Problem of Civilian Participation in Cyber Operations*

As described above, despite the ICRC's best efforts, an influential group of states consider the *Interpretive Guidance* to be "too rigid and complex, and [failing to] give an accurate picture of State practice or (in some respects) of a practice to

---

[139] DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.3 (citing NILS MELZER, THIRD EXPERT MEETING ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES: SUMMARY REPORT 35 (2005) ("Since, currently, the qualification of a particular act as direct participation in hostilities often depends on the particular circumstances and the technology or weapons system employed, it is unlikely that an abstract definition of direct participation in hostilities applicable to every situation can be found.").

[140] DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.3.1–5.8.3.2.

[141] *Id.* §5.8.4 (*citing* Nils Melzer, *Background Paper—Direct Participation on Hostilities under International Humanitarian Law—Expert Meeting of Oct. 25–26, 2004* 35 (discussing the wide range of opinions on the temporal scope of direct participation in hostilities).

[142] *Id.* §5.8.4. Again, the "revolving door" describes when a civilian repeatedly directly participates in hostilities, then ceases in order to regain immunity from attack, and then directly participates again when advantageous. *See supra* note 106–109.

[143] DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.4.2. *See also* Mack & Reeves, *supra* note 54, at 378 (discussing a similar legal inequity in reference to the continuous combat function analysis).

[144] *See* DOD LAW OF WAR MANUAL, *supra* note 11, §5.8.4.2.

[145] *Id.* §5.8.4. The U.S. approach to the "revolving door" situation is emphatic and clear: the LOAC gives no "revolving door" protection. As noted in the DOD Law of War Manual, "persons who are assessed to be engaged in a pattern of taking a direct part in hostilities do not regain protection from being made the object of attack in the time period between instances of taking a direct part in hostilities." *See* §5.8.4.2.

which States could realistically aspire."[146] In the alternative, these states take a more flexible approach to deciding whether a civilian is directly participating in hostilities in order to reflect the realities of the contemporary battlefield. Regardless which perspective is correct, this lack of unanimity makes determining when a civilian loses immunity from attack very difficult.

This analysis becomes even more complicated when trying to characterize a civilian's actions when participating in cyber space.[147] The ability to execute operations remotely is a key characteristic of the cyber domain, as the participating individual does not deploy. With no "geographic displacement," the "duration of direct participation in hostilities will be restricted to the immediate execution of the act and preparatory measures forming an integral part of that act."[148] Undoubtedly, complying with the principle of distinction in this new domain of warfare is immensely challenging.[149] Yet, the ever-increasing prevalence of civilian actors in cyber operations makes a direct participation in hostilities determination critical. For this reason, the analysis of the *Tallinn Manual 2.0*—which provides a comprehensive overview of the current state of international law as it pertains to cyber operations[150] —is helpful.[151]

IV. Tallinn Manual 2.0 on Direct Participation in Hostilities

Rule 97 of the *Tallinn Manual 2.0*, derived from Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II,[152] states: "[c]ivilians enjoy

---

[146] Pomper, *supra* note 13, at 186.

[147] *See supra* part III.B.

[148] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 53.

[149] *See* Michael W. Meier, *Emerging Technologies and the Principle of Distinction: A Further Blurring of the Lines between Combatants and Civilians*, *in* LIEBER SERIES VOL. 2 THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT 226–30 (Eric T. Jensen & Ronald T.P. Alcala eds., 2020) (discussing the difficulty of complying with the principle of distinction in cyber operations).

[150] In an effort to provide better understanding of the current state of international law as it pertains to cyber warfare, in 2009, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) located in Tallinn, Estonia, commissioned a three-year research project to examine the law of cyber conflict. The NATO CCD COE is a multinational and interdisciplinary center of cyber defence expertise. *See* NATO CCD COE, ABOUT US, https://ccdcoe.org/about-us/ [https://perma.cc/E8JE-EMDY] (last visited Feb. 22, 2019). That effort brought together an International Group of Experts (IGE) assisted by technical advisers with observers from the ICRC, the United States Cyber Command, and NATO. *See* Michael N. Schmitt, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, 48 ISR. L. REV., 81 (2015). In 2013, the final product of their efforts was published as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. *See generally* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2013). Upon publication of the first *Tallinn Manual*, the NATO CCD COE commenced a follow-on initiative to expand the Manual by adding analysis on peacetime cyber operations. This work was undertaken by a new IGE which led to the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*). *See generally* Tallinn MANUAL 2.0, *supra* note 15. The *Tallinn Manual 2.0* superseded the first *Tallinn Manual*, and most importantly, must be understood as an objective restatement of the *lex lata* and does not include statements that reflect the *lex ferenda*.

[151] *See generally* TALLINN MANUAL 2.0, *supra* note 15.

[152] TALLINN MANUAL 2.0, *supra* note 15, at 428. See *supra* notes 33, 41, 45, 80–81 and

protection against attack unless and for such a time as they directly participate in hostilities."[153] While this statement is arguably non-controversial,[154] the IGE addresses many contentious questions it raises concerning direct participation in hostilities in the commentary to the rule.[155] The *Tallinn Manual 2.0*, while non-binding,[156] provides persuasive and much needed clarity on when a civilian forfeits protection from attack in cyber operations.

A. Qualifying for Direct Participation in the Cyber Context

One important preliminary matter, addressed early in the commentary to Rule 97, is that, in the cyber context, a civilian must perform an act in order to constitute direct participation.[157] At first glance, this seems to be a statement of the obvious; however, the complexities and nature of cyber warfare may, in some cases, confuse the understanding of what constitutes an "act." For example, some individuals have the ability to hijack another person's computer, as part of a botnet attack, without the owner's knowledge or consent.[158] In this situation, the unwitting computer owner, despite the use of their computer in a cyber-operation, has not directly participated in hostilities.[159]

As to what acts qualify as direct participation in hostilities, the IGE generally agreed with the three constituent elements from the ICRC's *Interpretive Guidance* but held differing views as to their precise application in given circumstances. Regarding the threshold of harm, the IGE noted that there was no requirement for physical damage to objects or harm to individuals to satisfy the element.[160] For instance, a cyber operation that only alters data in the targeted computer system, may meet the threshold of harm element, provided that it negatively affects the enemy militarily.[161] Illustrating such circumstances, Marco

---

accompanying text on whether the rule also reflects customary international law in international and non-international armed conflicts.

[153] TALLINN MANUAL 2.0, *supra* note 15, at 428.

[154] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, §5.8 ("Civilians who take a direct part in hostilities forfeit protection from being made the object of attack.").

[155] TALLINN MANUAL 2.0, *supra* note 15, at 428–32.

[156] *See* Schmitt, *supra* note 127, at 799 (highlighting that only states can "reject, revise, or supplement" the law of armed conflict or "craft new norms"); Pomper, *supra* note 13, at 191 ("[I]t will be State practice—rather than international expert groups or the courts of any one country—that will drive the development of a common view within the international community.").

[157] *See* TALLINN MANUAL 2.0, *supra* note 15, at 429.

[158] *See* Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163, 167 (2014). Essentially, a botnet is network of computer systems infected with malware that permit hackers to remotely control them. *Id*. These hackers can then gain unauthorized access into the systems to engage in a number of nefarious activities. *Id*.

[159] TALLINN MANUAL 2.0, *supra* note 15, at 429. This vignette raises several other questions outside the scope of this article. For example, the computer itself may qualify as a targetable military objective. *See* AP I, *supra* note 5, art. 52(2) (defining military objective); TALLINN MANUAL 2.0, *supra* note 15, at 435–36. Or, "bots will often be located in at least some neutral States during an international armed conflict" potentially triggering protections for neutral critical infrastructure. *See id.* at 555.

[160] TALLINN MANUAL 2.0, *supra* note 1515, at 429.

[161] *Id*.

Roscini notes that cyber operations on "data in a military database containing deployment plans of the enemy's armed forces, [that] disrupts the command and control system of the enemy or shuts down the operating system of unmanned aerial vehicles so that they cannot be employed . . . reach the threshold of [] harm . . . even if no physical damage occurs."[162]

Additionally, some IGE members took the expansive position that the threshold of harm element is satisfied by those acts enhancing one's own military capacity, as these also undermine or negatively impact the enemy.[163] An example of such an act would be a civilian maintaining passive cyber defenses of military cyber assets as a capacity-enhancing act.[164] Underlying this broader interpretation is the belief that "restricting the threshold element to negative consequences for the enemy, when considered in light of the directness constitutive element, further risks an overly narrow interpretation of direct participation."[165] In other words, if a civilian is performing acts that add to the military capacity or capability of any party to an armed conflict, that conduct could rationally and reasonably harm an adversary and reach the necessary threshold of harm. Even if one accepts this conclusion, we believe the elements are *cumulative* in nature and the act still must meet the direct causation and belligerent nexus requirements to qualify as direct participation.

Considering the direct causation element, the IGE provided several cyber-specific examples to illustrate what is necessary to satisfy the requirement. Most obviously, the direct causation element is met if a civilian conducts a cyber-attack related to an armed conflict.[166] Extending the causal link further, the IGE opined that making cyber-attacks possible through specific acts, such as identifying vulnerabilities or designing malware to exploit such defects, would unambiguously amount to direct participation.[167] However, a civilian that designs malware and makes it openly available on the internet does not satisfy direct causation and, therefore, does not directly participate in hostilities even if the technology is used to harm the enemy.[168] Of course, the divide between direct and indirect causation is not entirely clear. An example of this ambiguity occurs when a civilian designs

---

[162] ROSCINI, *supra* note 91, at 205.

[163] TALLINN MANUAL 2.0, *supra* note 15, at 429. On a related point, the ICRC's *Interpretive Guidance* makes clear that a civilian's conduct does not meet the threshold of harm simply because he fails or refuses to positively affect an enemy. *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 66, at 49 ("[T]he refusal of a civilian to collaborate with a party to the conflict as an informant, scout or lookout would not reach the required threshold of harm regardless of the motivations underlying the refusal.").

[164] *Id.*

[165] Schmitt, *supra* note 126, at 720.

[166] The *Tallinn Manual 2.0* uses the term cyber-attack as a term of art. Rule 92 provides that "[a] cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destructions to objects." TALLINN MANUAL 2.0, *supra* note 15, at 415, 430.

[167] *Id.* at 430. The authors also state that gathering information on enemy operations via cyber capabilities and sharing that information with one's own armed forces would amount to direct participation. *Id*.

[168] *Id*.

and supplies malware, knowing that it will be used to conduct an attack, but does not know the particulars of the attack (*i.e.*, when and where it will occur).[169] Nevertheless, the IGE was divided on the question of direct causation in these types of circumstances,[170] leaving determinations to a case-by-case basis.[171]

Regarding the belligerent nexus element, the IGE noted that purely criminal or private acts occurring contemporaneously with the armed conflict are not sufficient to meet the element.[172] Of course, if the proceeds of a cybercrime are linked to the funding of a particular military operations, a belligerent nexus would likely exist.[173] But, a civilian committing a cybercrime against enemy military property or personnel does not *per se* establish a belligerent nexus as these acts may be done for purely personal gain unrelated to the armed conflict.[174]

B. The Commentary's Take on "For Such Time As"

Beyond the constituent elements of direct participation, the IGE wrestled with the topic of when direct participation begins and ends in the context of a cyber operation. As mentioned previously, the significance of determining this timeframe is that the individual remains targetable under the LOAC.[175] The IGE unanimously agreed that the period of direct participation at least covers conduct immediately before and after the qualifying act.[176] Some of the experts were comfortable extending "for such time" as far up or downstream as the causal link exists.[177]Acts at the beginning of this period may include penetrating, exploring, and gathering intelligence on a targeted system via cyber capabilities in order to look for defects exploitable in future operations.[178] After the qualifying act(s), some of the IGE

---

[169] *Id*.
[170] *Id*.
[171] *See* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 166 (2012).
[172] TALLINN MANUAL 2.0, *supra* note 15, at 430. This is not to say that cybercrime is not particularly problematic for States as:

> [T]echnology has created an extraordinary moment for industrious criminals, increasing profits without the risk of street violence. Digital villainy can be launched from faraway states, or countries, eliminating physical threats the police traditionally confront. Cyber perpetrators remain unknown. Law enforcement officials, meanwhile, ask themselves: Who owns their crimes? Who must investigate them? What are the specific violations? Who are the victims? How can we prevent it?

Al Baker, *An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported,* N.Y. TIMES (Feb. 5, 2018), https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html [https://perma.cc/D4W9-5JEW] (last visited Oct. 22, 2020).
[173] *See* TALLINN MANUAL 2.0, *supra* note 15, at 430–31.
[174] Schmitt, *Deconstructing Direct Participation in Hostilities*, *supra* note 126, at 735.
[175] *See* ROSCINI, *supra* note 91, at 209. It is worth noting that outside the timeframe for direct participation, lethal force is still permissible but under law enforcement standards for the use of force.
[176] *See* TALLINN MANUAL 2.0, *supra* note 15, at 431.
[177] *Id.*
[178] *See id*.

reasoned the period extends to include assessments to determine if another operation is necessary.[179] A complicating factor in determining with precision the period of direct participation in the context of cyber operations is time-delayed effects, such as the use of a piece of code that activates to perform a malicious function at a point in time after the initial insertion into a software system.[180] A majority of the IGE believed the period of participation started with "the beginning of his involvement in mission planning to the point when he or she terminates an active role in the operation."[181] Under these circumstances, the prejudicial effects to the system caused by the activation of the logic bomb may occur *after* the individual who was responsible for inserting it was no longer directly participating in hostilities.[182]

A minority of the IGE considered emplacement and activation by the same person as "separate acts of direct participation."[183] Under this bifurcated approach, "the completion of emplacement would end the first period of direct participation and taking steps later to activate the logic bomb would mark the commencement of a second period."[184] As a variant to this issue, the IGE delved into the circumstance where an individual launches repeated cyber operations over an extended period all of which amount to qualifying acts of direct participation.[185] Again, the IGE was divided in its analysis of this situation.[186] Some of the experts reasoned that each incident stood alone as an act of direct participation, and, as such, the individual is targetable only during the specific periods of participation and not during the periods in between.[187] Others believed such an approach made "little operational sense" seeing it as an example of the "revolving door," and the actor is targetable for the duration of the entire period.[188]

C. Legal Fault Lines

The final issue addressed by the IGE was whether a presumption against direct participation is applicable. This discussion and debate related, in part, to the provision codified in Article 50(1) of Additional Protocol I, which provides "[i]n case of doubt whether a person is a civilian, that person shall be considered a civilian."[189] This issue split the IGE; the Commentary to Rule 97 articulated the opposing positions as follows:

---

[179] *Id*.
[180] *Id.*
[181] *Id*.
[182] *Id*.
[183] *Id.*
[184] *Id*. at 431–32. Benjamin Weitz, *Updating the Law of Targeting for an Era of Cyberwarfare*, 40 U. PA. J. INT'L L. 735, 746 (2019). A logic bomb is malicious code that activates once a condition is met, when a specified event occurs, or at a certain time and date. *Id*.
[185] *See* TALLINN MANUAL 2.0, *supra* note 15, at 432.
[186] *Id*.
[187] *See id.*
[188] *Id*.
[189] AP I, *supra* note 55, art. 50(1).

> Some Experts took the position that, in case of doubt, as to whether a civilian is engaging in an act of direct participation (or as to whether a certain type of activity rises to the level of direct participation), a presumption against direct participation attaches. Other Experts objected to the analogy to Rule 95 (regarding the presumption in cases of doubt as to status). They were of the view that when doubt exists, the attacker must, as a matter of law, review all of the relevant information and act reasonably in the circumstances when deciding whether to conduct the attack. No presumption attaches.[190]

The lack of consensus among the IGE on the presumption question is not surprising.[191] However, it also indicates that there remain a number of unresolved legal questions—or *fault lines*—concerning direct participation in hostilities during cyber operations. Further exploring these fault lines is therefore a helpful exercise

---

[190] *See* TALLINN MANUAL 2.0, *supra* note 15, at 432 (citation omitted).

[191] Whether there is a legal presumption of civilian status in cases of doubt is a contentious topic among scholars and States. *See, e.g.*, RULES, *supra* note 11, at 23–4 (discussing various State perspectives on situations of doubt as to the character of a person); *compare* DOD LAW OF WAR MANUAL, *supra* note 11, §5.4.3.2. (stating that "[a] legal presumption of civilian status in cases of doubt may demand a degree of certainty that would not account for the realities of war"), *with* U.K. MANUAL, *supra* note 32, §5.3.4 (2004) ("In the practical application of the principle of civilian immunity and the rule of doubt, (a) commanders and others responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is available to them at the relevant time, (b) it is only in cases of substantial doubt, after this assessment about the status of the individual in question, that the latter should be given the benefit of the doubt and treated as a civilian, and (c) the rule of doubt does not override the commander's duty to protect the safety of troops under his command or to preserve the military situation."), *and* Argentina, LAW OF WAR MANUAL (1989), §4.02(1) ("[I]n case of doubt about the qualification of a person, that person must be considered to be a civilian."), *and* Australia, DEFENCE FORCE MANUAL (1994), §914 ("[I]n cases of doubt about civilian status, the benefit of the doubt is given to the person concerned."), *and* Cameroon, INSTRUCTORS' MANUAL (1992), at 17 ("[T]he benefit of the doubt confers upon a person the status of civilian."), *and* Canada, LOAC MANUAL (1999), at 4–5, §38 ("[I]n case of doubt whether a person is a civilian, that person shall be considered to be a civilian."), *and* Colombia, INSTRUCTORS' MANUAL (1999), at 16 ("in case of doubt whether a person is civilian or not, that person must be considered to be a civilian."), *and* Kenya, LOAC MANUAL (1997), Pre´cis No. 2, at 10 ("[I]n case of doubt whether a person is a civilian or not, that person shall be considered a civilian."), *and* Sweden, IHL MANUAL (1991), §3.2.1.5, at 42 ("[W]here there is doubt whether a person is to be considered a combatant or as a civilian, the person shall be considered as a civilian."), *noted in* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: VOLUME II: PRACTICE – PART 1, 130–32 (2005). A similar debate concerns the characterization of objects. *See, e.g.*, INT'L COMM. OF THE RED CROSS, *Rule 10: Civilian Objects' Loss of Protection from Attack*, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule10 [perma.cc/5LD4-2SR4] (last visited Aug. 29, 2019) ("The issue of how to classify an object in case of doubt in not entirely clear."); DOD LAW OF WAR MANUAL, *supra* note 11, §5.4.3.2 ("Under customary international law, no legal presumption of civilian status exists for persons or objects, nor is there any rule inhibiting commanders or other military personnel from acting based on the information available to him or her in doubtful cases.") (citing Christopher Greenwood, *Customary International Law and the First Geneva Protocol of 1977 in the Gulf Conflict*, *in* PETER ROWE, THE GULF WAR 1990–91 IN INTERNATIONAL AND ENGLISH LAW 63, 75 (1993)).

in conceptualizing and understanding the practical application of the current direct participation legal standard in the ambiguous cyber domain.

It is worth reiterating that the notion of direct participation in hostilities has historically been one of, if not the, most vexing provision in the regulation of conventional battlefield conduct.[192] Cyber operations clearly make the normatively challenging issue of direct participation under the LOAC even more complex. The commentary to rule 97, summarized above, is helpful in identifying the most difficult issues regarding direct participation in hostilities in a cyber context. Therefore, it is worthwhile to examine the IGE's disagreements to develop an understanding for how this complicated topic can apply in practice.

1. Temporal Scope of Cyber Operations

The first cyber-related fault line highlighted in the commentary to Rule 97 is temporal. Stated differently, how long is the period of direct participation such that the individual involved in a cyber operation is lawfully targetable under the LOAC? The phrase "for such time" in Rule 97 vaguely identifies or constrains the period in question. Understandably, the IGE was split in its analysis with unanimity only on the period immediately before and after the qualifying act. In some respects, the temporal limitation, for all practical purposes, makes targeting a direct cyber participant highly problematic, as cyber actors are incredibly difficult to identify with certainty.[193] Stealth, anonymity, and deception are but a few of the defining characteristics of cyber operations. The qualifying acts may sometimes last only minutes whereas the system administrators and cyber security experts on the receiving end may not realize for an extended period that they were the target of a cyber operation. Thus, in many cases, the notion of targeting an individual during the period of participation is limited to an academic exercise, as there is no realistic window for the victim of the cyber operation to attack the perpetrator.[194]

Relatedly, many cyber operations are time-delayed and involve technologies like a logic bomb that make it extremely difficult to determine when direct participation begins and ends.[195] The very nature of these operations is characterized by a period of time, which may be significant, between the insertion of the malicious software in a system and its activation and corresponding effects.[196] In considering direct participation in these categories of cases, while the IGE was again divided in its analysis, Roscini generally addressed such a scenario, stating:

---

[192] *See* sources cited *supra* note 190.
[193] *See generally* David A. Wallace & Christopher W. Jacobs, *Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines*, 40 U. PA. J. INT'L L. 643, 682–84 (2019) (discussing the challenges of attribution in cyber).
[194] *Cf.* Schmitt, *supra* note 82, at 14 (making a similar observation in the kinetic context).
[195] Weitz, *supra* note 184.
[196] *See id.*

> In particular, one fails to see the military necessity of attacking someone who is not playing any longer a role in the operation: the act of hostilities may well continue, but the direct participation would not. Referring to the notion of continuing act to justify an extension of the duration of participation in hostilities so to also cover the effects of the act is not helpful.[197]

Roscini's approach is consistent with the majority of the IGE and is intuitively reasonable. It is important to note that even though such a civilian would not be targetable for a time-delayed act of hostility, he or she may still be subject to criminal prosecution.

Finally, some individuals execute repeated cyber operations over an extended period with all being qualifying acts of direct participation. In these situations, the "for such time" clause covers the entire period of repeated cyber operations.[198] That is, the continuous nature of repeated cyber operations makes the individual targetable so long as the operations continue, as if the individual were holding the revolving door continuously open. As a practical matter, the longer the individual engages in the repeated acts of direct participation, the more likely the victim state will be able to identify and strike those directly participating. And, unlike Roscini's previous argument, military necessity permits the targeting of an individual who is repeatedly and consistently engaging in hostile cyber operations.[199]

2. The Direct Causation Challenge

As mentioned previously, the constituent element dictates that there must be a direct causal link between the civilian's specific act and the likely harm. In an effort to help clarify this concept, the ICRC's *Interpretive Guidance* states that the directness of the link must occur in one causal step to differentiate between direct and indirect participation.[200] Expanding on this point, the *Interpretive Guidance* added that it is not sufficient that the qualifying act and its consequences be linked through an interrupted causal chain of events.[201] Some States and scholars reject the strict "one causal step" analysis and take a more contextual approach to

---

[197] ROSCINI, *supra* note 91, at 209.

[198] This analysis is significantly easier for those States that reject the "revolving door" analysis and instead make the direct participation determination is on a case-by-case analysis. *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 11, §5.9.4.

[199] Some of the IGE assert in the discussion of Rule 97 that direct participation begins with the first cyber operation and continues throughout the period of intermittent activity, impliedly suggesting that military necessity permits targeting such participants. *See* TALLINN MANUAL 2.0, *supra* note 15, at 432.

[200] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 42. The second part of the direct causation element which states "or from a coordinated military operation of which that act constitutes an integral part," seems to address the one causal step issue. DINNISS, *supra* note 171, at 166. Of course, if the actions of the individual were not part of a coordinated military operation that portion of the direct causation element simply would not apply.

[201] ICRC INTERPRETIVE GUIDANCE, *supra* note 66, at 42, 52–58.

determining causation.[202] Regardless of the approach, it is extremely difficult to determine, with any degree of precision, the causal link between the qualifying act and resulting harm in the context of a cyber operation. This difficulty is driven by the fact that many cyber operations create a domino-like effect, with the physical consequences or manifestations being indirect. For example, cyber weapons produce a different variety of effects in the digital domain. Not surprisingly, the direct effects are the targeting of computers and related networks. These include the deletion, corruption, or alteration of data or otherwise disrupting an enemy's computer networks.[203] On the other hand, the secondary effects may involve the destruction or incapacitation of cyber infrastructure.[204] Lastly, tertiary effects, such as the loss of electrical power or water due to a cyber operation that targets a power plant or water filtration facility, are the impacts on those persons affected by the secondary effects.[205]

The cyberattack against a Ukrainian power grid in December 2015, affecting the electric power for 225,000 customers, is an example of such a domino-effect.[206] The direct effect of the attack was to the power company's computers and related networks. The secondary effect involved any destruction or incapacitation of the company's cyber infrastructure, particularly the supervisory control and data acquisition network. Finally, the tertiary effects fell on the customers who lost electrical power.

Admittedly, the direct causation element can be challenging when applied to cyber operations. When considered through the lens of the *Interpretive Guidance,* applying this element becomes particularly problematic because of the ICRC's overly restrictive characterization of the link between the qualifying act and its consequences, *i.e.*, "one causal step."[207] Therefore, it seems that the "case-by-case" or "contextual" approach taken by the United States and others is arguably more operationally palatable as it provides the necessary flexibility for determining whether a particular cyber operation would amount to a direct participation in hostilities.[208]

3. The Irrelevance of Geography in Cyber Operations

---

[202] *See* Schmitt, *supra* note 82, at 29–30 ("The Interpretive Guidance's explanation of directness is strict on its face, arguably overly so . . . [and] [t]he reference to 'one casual step' is unfortunate . . . .").
[203] ROSCINI, *supra* note 91, at 169.
[204] *Id*.
[205] *Id*. at 53 ("Physical damage to property, loss of life and injury to persons, then, are never the primary effects of a cyber operation: damage to physical property can only be a secondary effect, while death or injury of persons can be a tertiary effect of a cyber operation.").
[206] *See* Wallace & Reeves, *supra* note 129, at 1611.
[207] *See supra* notes 198–204 and accompanying text.
[208] *See id*. *See also* Schmitt, *supra* note 82, at 38 ("The better approach is one whereby a civilian who directly participates in hostilities remains a valid military objective until he or she unambiguously opts out of hostilities through extended non-participation or an affirmative act of withdrawal.").

While not expressly discussed by the IGE in the commentary to Rule 97, a third implied fault line is whether a civilian, geographically remote from an armed conflict, is considered to be directly participating if they are responsible for a related cyber-attack.[209] Cyber operations are often far removed from the location of the effects. In fact, the ability to conduct operations remotely is one of the most alluring features of cyber means and methods.[210] Yet, from a traditional perspective, "geographic proximity to the battle lines has also been used as a rough guide to ascertaining the status of the civilian concerned . . . ."[211]

However, modern military systems like cyber weapons make the geographical location of the participant relative to the qualifying act irrelevant. Validating this position, the Israeli Supreme Court in its *Targeted Killing* opinion found that a person, despite considerable distance from the battlefield, directly takes part in hostilities if they operate, supervise the operation, or service a system.[212] From a practical perspective, this is the better approach as cyber operations are often "launched far from the active battlespace" and can come "from any location where connectivity to the target cyber system can be established."[213] Therefore, the IGE's finding that "[a]ny act of direct participation in hostilities by a civilian renders that person targetable for such time as he or she is engaged in the qualifying act"[214] seems to rest on the assumption that these types of determinations are made irrespective of where the civilian is located.

4. Revisiting the Presumption Against Direct Participation

A final fault line, as highlighted in the previous section, is whether there exists a presumption against direct participation.[215] This issue, when considered broadly, is at the fulcrum between military necessity and humanity, and speaks to the legal lens for accessing ambiguous status. The IGE, for their part, in rule 95 of the *Tallinn Manual—Doubt as to status of person*,[216] articulated a position that states "[i]n case of doubt as to whether a person is a civilian, that person shall be considered a civilian."[217] The IGE found this rule reflected customary international

---

[209] How an individual is targeted away from a "hot battlefield" is outside the scope of this article. For a discussion on this topic, *see generally* Shane R. Reeves, Winston Williams & Amy H. McCarthy, *How Do You Like Me Now? Hamdan v. Rumsfeld and the Legal Justifications for Global Targeting*, 41 U. PA. J. INT'L L. 329 (2020).

[210] *See generally* CLAIRE FINKELSTEIN & KEVIN GOVERN, *Introduction: Cyber and the Changing Face of War*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS x–xi (Jens David Ohlin, Kevin Govern, & Claire Finkelstein eds., 2015), https://scholarship.law.upenn.edu/faculty_scholarship/1566 [https://perma.cc/4Z5V-LXUG] (last visited Oct. 24, 2020).

[211] DINNISS, *supra* note 171, at 164.

[212] *See* HCJ 769/02 Pub. Comm. Against Torture in Isr. v. Gov't of Isr. (Targeted Killings) PD 62(1) 507, ¶ 37 (2006) (Isr.).

[213] *See* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 288–89 (2014).

[214] TALLINN MANUAL 2.0, *supra* note 15, at 431.

[215] *See supra* notes 206–209 and accompanying text.

[216] TALLINN MANUAL 2.0, *supra* note 15, at 424.

[217] *Id*.

law, applied to both international and non-international armed conflicts, and was further codified in Article 51(1) of Additional Protocol I.[218] In contrast, the United States, in its *Law of War Manual*, maintains that the presumption of civilian status is not a part of customary international law and therefore commanders may act based on available information in doubtful cases.[219]

In regard to direct participation and whether a presumption of doubt attaches to a civilian engaging in questionable acts, the IGE split into the two camps described above.[220] Despite this disagreement, the commentary implies that all experts agreed that the issue of doubt is particularly important when determining direct participation in the context of cyber operations. This makes sense for several reasons. First, the use of computers and computer infrastructure by civilians is ubiquitous, as millions of persons spread across the globe innocently enter the virtual domain on a daily basis.[221] Second, individuals that engage in cyber operations are deliberately attempting to conceal their identity, and the consequences of their acts may be time-delayed or geographically remote from the qualifying act for direct participation.[222] Third, the armed forces often, and increasingly so, use civilian computer networks.[223]

Clearly, there remains much doubt and ambiguity regarding a civilian's status when conducting cyber operations. That ambiguity is one of its defining characteristics of cyber operations and is the reason making a direct participation determination is so difficult. This dilemma is not easily resolved as those States operating in this space are likely to want to protect their own civilian population while aggressively targeting those of their adversaries. For this reason, though unsatisfying, "[i]t is unclear how this classic military necessity/humanity conflict will be resolved" going forward.[224]

V. Conclusion

The legal complexities and practical difficulties of applying the rule and concept of "taking a direct part in hostilities" under the LOAC is extraordinarily challenging. When viewing the topic of direct participation in hostilities through the lens of cyber operations, it makes its application even more difficult. Moreover, these difficulties show no evidence of abating, considering the prevalence of

---

[218] *Id*. However, the precise threshold of doubt necessary to trigger a presumption of civilian status is unsettled under the LOAC, *see id.*
[219] DOD LAW OF WAR MANUAL, *supra* note 11, §5.4.3.2.
[220] *See* TALLINN MANUAL 2.0, *supra* note 15, at 432.
[221] *See* TALLINN MANUAL 2.0, *supra* note 15, at 424 ("In many countries, the use of computers and computer networks by civilians is pervasive . . . .").
[222] *See id.* at 431.
[223] *Id.* at 424. ("[T]he networks that civilians and the armed forces use may be conjoined."); Schmitt, *supra* note 213, at 298–99 (discussing the increasing reliance on dual-use cyber infrastructure by global military forces).
[224] Schmitt, *supra* note 213, at 299.

civilians operating in the virtual domain coupled with the inherent challenges of cyber operations.

However, the IGE took the important first step in addressing this issue by articulating a reasonable view on the *lex lata* with respect to civilians taking a direct part in hostilities in the context of cyber operations. In doing so, the IGE does a great service by illustrating the fault lines that exist when conducting a direct participation analysis in the context of cyber operations. Consequently, the IGE's work has made it easier to understand why states are struggling to comply with the principle of distinction in this new domain of warfare. Hopefully, this article has built upon the IGE's work by exploring the divisive issues embedded in rule 97 of *Tallinn Manual 2.0* and help close those legal gaps that are so easily exploited in the current LOAC framework during cyber operations.