International Review of the Red Cross (2023), **105** (923), 965–991.
Organized crime
doi:10.1017/S1816383123000152

IRRC

Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield

Kubo Mačák*
Legal Adviser, International Committee of the Red Cross, Geneva
Email: kmacak@icrc.org

Abstract

This article argues that the growing involvement of civilians in activities on the digital battlefield during armed conflicts puts individuals at risk of harm and contributes to the erosion of the principle of distinction, a cornerstone of international humanitarian law (IHL). The article begins by outlining the ongoing trend of civilianization of the digital battlefield and puts forward brief scenarios to illustrate it. It then examines the narrow circumstances under which such forms of civilian involvement may qualify as direct participation in hostilities under IHL, and discusses what this means for the individuals concerned, particularly from the

* Earlier versions of this article were presented at the American University's symposium on "The Evolving Face of Cyber Conflict and International Law" in June 2022 in Washington, DC, and at the University of Oxford's conference on "How International Law Applies in Cyberspace" in October 2022. I am grateful to the participants at both events for their helpful comments. I would also like to expressly thank Ana Beduschi, Lindsey Cameron, Cordula Droege, Laurent Gisel, Jonathan Horowitz, Vanessa Murphy, Tilman Rodenhäuser and Mauro Vignati for their feedback on earlier drafts, as well as Julio Veiga-Bezerra for his research assistance.

perspective of their loss of protection under the law. The analysis shows that certain types of State conduct which put civilians in harm's way by inducing them to directly participate in hostilities may constitute standalone violations of IHL and human rights law obligations. Beyond these specific prescriptions, the encouragement of civilian involvement undermines the principle of distinction, with dangerous ripple effects on the interpretation of those rules of IHL that flow from it. Accordingly, the article concludes that States should act to reverse the trend of civilianization of the digital battlefield and refrain as much as possible from involving civilians in the conduct of cyber hostilities.

Keywords: armed conflict, civilians, cyber operations, direct participation in hostilities, international humanitarian law.

Introduction

The principle of distinction is right at the centre of international humanitarian law (IHL). Woven deep into the fabric of this body of law, it is the material from which many of its rules are made. By prescribing that parties to armed conflicts must at all times distinguish between civilians and combatants and between civilian objects and military objectives, it draws a firm line of protection around those persons and objects that must be spared, as much as possible, from the effects of hostilities.

With the ongoing digitalization of warfare, however, the principle of distinction has come under renewed pressure. It has never been easier to involve civilians in military cyber and digital activities – and it has never been easier to harm them through these means. Most alarmingly, some behaviours of parties to armed conflicts may bring about both of these consequences at the same time. Can the law keep pace with these developments? And can the centre of IHL withstand the pressure that they bring?

This article argues that States and parties to armed conflicts more generally should refrain from involving civilians in the conduct of cyber hostilities, for important reasons of law and policy. Its principal contention is that it is not too late to reverse the damaging trend of the erosion of the principle of distinction in the cyber context, but it is essential that we recognize what is at stake and take action now. In order to build this argument, the article proceeds in five consecutive steps.

First, the article outlines the ongoing trend of civilianization of the digital battlefield and puts forward three brief scenarios to illustrate it. Second, the article examines the narrow circumstances under which such forms of civilian involvement may qualify as direct participation in hostilities under IHL. Third, it explores what this means for the individuals concerned, particularly from the perspective of their loss of protection under the law. Fourth, it analyzes the legal implications for States that engage in such conduct, under both IHL and human rights law. Finally, the article ends with an overall conclusion and recommendations for States.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Civilianization of the digital battlefield

From general trends to qualitative and quantitative shifts in the digital space

One of the fundamental premises of IHL is the separation of all persons affected by an armed conflict into two generic categories: on the one hand, there are the combatants, who conduct the hostilities on behalf of the parties to the conflict, and on the other hand, there are the civilians, who are presumed to refrain from doing so and who must therefore be protected against the dangers arising from the conflict.[1]

The line between these two categories has never been fully impermeable, and civilians have been used to perform military functions during armed conflicts and to assist in the war effort since time immemorial.[2] Yet, for most of human history this involvement has typically been fairly minimal or limited to indirect forms of support such as "the production or provision of arms, equipment, food and shelter, [or] economic, administrative and political support".[3]

This is no longer the case today. Private contractors, civilian intelligence personnel and other civilian government employees are increasingly involved in military operations. The urbanization of warfare has brought conflict literally onto individual civilians' doorsteps, with many of them taking on active roles in the fighting. In asymmetrical conflicts in particular, the nominally weaker side will often engage and rely on civilians to confuse and outmanoeuvre the asymmetrically stronger enemy.[4]

In addition, the ongoing process of digitalization has enabled certain novel qualitative and quantitative shifts. From the qualitative perspective, digital forms of involvement have a much lower threshold – with some degree of exaggeration, it can be said that anyone with a smartphone is capable of joining in. Digitalization has also erased, or transformed, the concept of remoteness: while individuals may be physically remote from the theatre of hostilities, they are only a few clicks away from the digital battlefield.

1 This article focuses on situations of international armed conflict and the law applicable to that type of armed conflict. While the concept of "combatants" is limited to international armed conflicts, the principle of distinction is applicable to all types of armed conflict. Much of the analysis in this article can thus be applied *mutatis mutandis* to situations qualifying as non-international armed conflict as well, but exploring the specific nuances of that context falls outside of its scope.

2 See David R. Meddings, "Civilians and War: A Review and Historical Overview of the Involvement of Non-Combatant Populations in Conflict Situations", *Medicine, Conflict and Survival*, Vol. 17, No. 1, 2001.

3 International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, 2007, p. 15. One historical exception is the *levée en masse* – i.e., the spontaneous uprising of the civilian population against the invading forces of the enemy. As documented in a recent study, this concept originated during the revolutionary wars in America and France, but there have been virtually no instances of *levée en masse* in modern armed conflicts: see Emily Crawford, "Tracing the Historical and Legal Development of the *Levée en Masse* in the Law of Armed Conflict", *Journal of the History of International Law*, Vol. 19, No. 3, 2017.

4 Andreas Wenger and Simon J. A. Mason, "The Civilianization of Armed Conflict: Trends and Implications", *International Review of the Red Cross*, Vol. 90, No. 872, 2008, p. 848.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

On the quantitative side, the characteristics of the digital space have made it much easier to scale up any civilian involvement. A group comprising thousands or even tens of thousands of individuals may be formed and coordinated in a matter of hours. Similarly, the attack surface of societies has vastly increased – there are digital devices, apps and networks everywhere, which means that in time of armed conflict, there are exponentially more vulnerabilities than in the wars of the past.

Three illustrative scenarios

Several examples – all drawing on incidents and activities reported during recent armed conflicts – may help illustrate these trends. First, States may encourage civilians to engage in offensive cyber operations against targets associated with the enemy (scenario 1). These kinds of involvement may range from the simplest forms, such as joining a distributed denial-of-service (DDoS) attack, to more complex ones, such as contributing to cyber operations aimed at disrupting enemy assets or infrastructure. Individual civilians can be easily mobilized and coordinated through digital means, and existing groups of "hacktivists" can be federated by States.[5] The outsourcing of military cyber operations to civilians may offer certain advantages such as lower costs and operational efficiency, but these must be weighed against the risks posed by the lack of training and discipline at the level expected from military personnel.

Second, States may repurpose existing e-government or other smartphone applications for military use (scenario 2). During an armed conflict, such applications can be "enhanced" by building in new functionalities to encourage users to contribute to the military effort by, for example, reporting the movements of enemy troops, vehicles or aircraft by uploading location-tagged images or videos.[6] Given that the apps are well understood by the population, their use does not require a training period; the new capabilities can be used immediately. For the State in question, an existing community of digital citizens familiar with a given app may present an opportunity to rapidly increase its capabilities in time of war. At the same time, the reliability, accuracy and ultimately operational value of information gathered in this way must be carefully assessed by the receiving State. As will be detailed later, another key disadvantage relates to the risk that the provision of the information poses to the civilians using the app.

5 See e.g. Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army", OpenNet Initiative, May 2011, available at: https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army (all internet references were accessed in April 2023); Stefan Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, Center for Security Studies, ETH Zürich, June 2022.

6 See e.g. Drew Harwell, "Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War", *Washington Post*, 24 March 2022, available at: www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/; Dan Sabbagh, "Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks", *The Observer*, 29 October 2022, available at: www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Third, either voluntarily or out of a domestic legal obligation, private companies – i.e., civilian entities – that control cyber infrastructure may defend against deliberate cyber attacks originating from abroad or share threat intelligence with government authorities such as national cyber defence entities (scenario 3). A key advantage of such activities for States is that they strengthen the national cyber resilience while offloading the costs for doing so to non-State actors. Even if the frameworks for such involvement are developed with peacetime contexts in mind, the cyber defence actions taken on their basis during armed conflicts may well in effect thwart or at least impede the enemy's military cyber operations. These forms of involvement may, however, invite retaliation by the enemy, which can not only directly endanger the staff and property of the concerned companies but may also negatively affect civilians and civilian services reliant on those companies.[7]

These three examples highlight different forms of civilian involvement as well as their key potential advantages and disadvantages from the military and policy perspectives. Some of them may be taken on the civilian actors' own initiative, while others may be encouraged by States or even mandated by the law. What all of them share, though, is that they draw civilians into a space that is normally occupied by the military, thus potentially blurring the line between civilians and combatants in cyberspace.[8]

This problem is not unknown to States, which have acknowledged its various facets in their official pronouncements. For instance, during recent multilateral discussions at the United Nations (UN), Russia has suggested that it is "very difficult (if not impossible) to draw a distinction in virtual space between … combatants and non-combatants".[9] Similarly, Japan has called for further discussions on how IHL rules on "the scope of combatants apply to cyberspace".[10] And in its 2021 national position on the application of international law in cyberspace, Brazil described the question of "when a civilian acting in the cyberspace might be considered as taking direct part in hostilities" as one of the key unsettled issues in IHL.[11] This is the question to which we will turn in the next section.

7 See, further, Jonathan Horowitz, "One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict", forthcoming.

8 For a legal perspective on the supposedly blurred line between combatants and non-combatants in cyberspace, see Kubo Mačák, "Unblurring the Lines: Military Cyber Operations and International Law", *Journal of Cyber Policy*, Vol. 6, No. 3, 2021, pp. 419–421, available at: www.tandfonline.com/doi/full/10.1080/23738871.2021.2014919.

9 Russia, "Statement by Dr. Vladimir Shin, Deputy Director of the Department of International Information Security of the Ministry of Foreign Affairs of the Russian Federation, at the Online Consultations of the Open-Ended Working Group on the Developments in the Field of Information and Telecommunications in the Context of International Security", 30 September 2020, p. 2.

10 Japan, "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations", 28 May 2021, p. 7.

11 Brazil, "National Contribution on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", in *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of*

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Cyber activities and direct participation in hostilities

General rule

Under IHL, civilians are protected against attack unless and for such time as they directly participate in hostilities. This rule is articulated in Article 51(3) of Additional Protocol I (AP I) and Article 13(3) of Additional Protocol II (AP II). It reflects customary international law applicable in both international and non-international armed conflicts.[12]

Importantly, not every form of civilian involvement in the war effort qualifies as direct participation in hostilities.[13] The cited treaty provisions do not contain more precise criteria and so far, no clear and uniform definition of direct participation in hostilities has been developed in State practice either.[14] However, the International Committee of the Red Cross (ICRC) has published an *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC Interpretive Guidance), according to which an act amounts to direct participation in hostilities if it meets the following three cumulative conditions:

1. 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
2. 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
3. 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).[15]

The ICRC's criteria have been described in international jurisprudence as "useful guidance".[16] While not all States are fully aligned with the tripartite test,[17]

International Security Established Pursuant to General Assembly Resolution 73/266, UN Doc. A/76/136, 13 July 2021, p. 23.

12 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rule 6, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1. See also Supreme Court of Israel, *The Public Committee against Torture in Israel and Others v. Government of Israel and Others*, HCJ 769/02, Judgment, 14 December 2006, para. 38.

13 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), p. 619, para. 1945.

14 ICRC Customary Law Study, above note 12, p. 23.

15 Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009 (ICRC Interpretive Guidance), p. 46.

16 International Criminal Court (ICC), *The Prosecutor v. Callixte Mbarushimana*, Decision on the Confirmation of Charges, 16 December 2011, para. 148.

17 Some are nonetheless very similar in their approaches: see e.g. Norway, *Manual i krigens folkerett*, 2013 (Norwegian Military Manual), paras 3.24–3.27 (relying on the criteria of (1) "damage or injury", (2)

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

several have expressly endorsed it, either in general terms or specifically in the cyber context, including Colombia (in general),[18] Denmark (in general),[19] France (specifically)[20] and Germany (specifically).[21] In the cyber context, it has also been endorsed by the international group of experts who drafted the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (Tallinn Manual 2.0).[22]

In the next subsection, we will return to the three scenarios mentioned earlier and assess them against the "analytical tools"[23] set out in the ICRC Interpretive Guidance. In practice, each activity must be carefully evaluated on a case-by-case basis against these criteria before a determination is made.[24] As will be seen, the cumulative criteria set the bar very high, and specific forms of civilian involvement clear it only in exceptional circumstances.

Application of the general rule to the three scenarios

Threshold of harm

In order for an act to meet the first criterion, it must be likely to adversely affect the military operations or capacity of the adversary, irrespective of the means used or of

"direct cause" and (3) "intent"). Military manuals of other States, several of which were drafted before the ICRC Interpretive Guidance, either do not examine the meaning of direct participation in hostilities or employ differently formulated legal tests: see e.g. Australia, *Law of Armed Conflict*, Australian Defence Force, Canberra, 2006, p. 5-10, para. 5.36; Canada, *The Law of Armed Conflict at the Operational and Tactical Levels: Joint Doctrine Manual*, Department of National Defence, Ottawa, 2001, p. 3-4, para. 28; New Zealand, *Manual of Armed Forces Law*, Vol. 4, New Zealand Defence Force, Wellington, 2019 (New Zealand Military Manual), pp. 6-15–6–17, paras 6.5.13–6.5.17; Spain, *Orientaciones: El derecho de los conflictos armados* [*Guidelines on the Law of Armed Conflict*], 2nd ed., Ministerio de Defensa, 2007, para. 5.2.a.(2)(a); Switzerland, *Bases légales du comportement à l'engagement* [*Regulation on Legal Bases for Conduct during an Engagement*], Swiss Army, 2005 (Swiss Military Manual), para. 197; United Kingdom, *The Manual of the Law of Armed Conflict*, Joint Service Publication 383, Ministry of Defence, 1 July 2004 (UK Military Manual), para. 5.3.3; United States, *Department of Defense Law of War Manual*, Office of General Counsel, Department of Defense (DoD), Washington, DC, June 2015 (updated December 2016) (DoD Military Manual), section 5.8.

18 Colombia, *Manual de derecho operacional* [*Operational Law Manual*], 2nd ed., Ministerio de Defensa Nacional, Comando General de las Fuerzas Militares, Santafé de Bogotá, 2015, p. 41.

19 Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Danish Ministry of Defence, Defence Command Denmark, 2016 (Danish Military Manual), pp. 168–169.

20 France, *International Law Applied to Operations in Cyberspace*, Ministry of the Armies, 2019 (French Position Paper), p. 13.

21 Germany, *On the Application of International Law in Cyberspace: Position Paper*, March 2021 (German Position Paper), p. 8.

22 Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 97, commentary para. 5.

23 Dapo Akande, "Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities", *International and Comparative Law Quarterly*, Vol. 59, 2010, p. 192.

24 See International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor v. Pavle Strugar*, Case No. IT-01-42-A, Judgement (Appeals Chamber), 17 July 2008, para. 178; ICC, *The Prosecutor v. Bahr Idriss Abu Garda*, Case No. ICC-02/05-02/09, Decision on the Confirmation of Charges, 8 February 2010, para. 83.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

whether it would reach the level of an attack on its own.[25] It does not necessarily have to qualify as an "attack" under IHL (the exact threshold of which is unsettled in the cyber context[26]) or involve the use of "weapons".[27] Accordingly, it is widely accepted that, for example, clearing mines placed by the enemy or wiretapping the enemy's communications could suffice depending on the situation, even though such activities do not amount to attacks in the IHL sense of the word.[28]

Offensive cyber operations against targets associated with the enemy, as envisaged in scenario 1, do not meet this criterion unless they may "negatively affect the enemy militarily".[29] In practice, this means that such operations would, if successful, reduce the military capacity of the enemy or at least interfere with the enemy's military operations. For example, a cyber operation against the computer network of a railway company in time of armed conflict could be designed to block the deployment of trains carrying military equipment belonging to the enemy, thus adversely affecting the enemy's operations.[30] However, not any manipulation of computer networks would suffice; adverse military effects must be at least likely at the time the operation is planned.[31]

Many forms of information about the enemy's movements provided to the military through a smartphone application – covered in scenario 2 – would be too general or insignificant to meet the "threshold of harm" criterion. In the traditional physical-world context, there is a "general agreement that civilians merely answering questions asked by passing military personnel could not be considered as directly participating in hostilities".[32] The same logic applies with regard to digital intelligence sharing. It is only if the information is essential for the execution of a specific military operation, such as transmitting tactical targeting information for an attack, that its provision may be considered

25 Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 5 ("actions that do not qualify as a cyber attack will satisfy this criterion so long as they negatively affect the enemy militarily"); but see United Kingdom, "Application of International Law To States' Conduct In Cyberspace: UK Statement", Foreign, Commonwealth and Development Office, 3 June 2021, para. 25, which seems to place the bar higher (i.e., at the level of attack).

26 For a recent overview of the debate, see e.g. Kubo Mačák and Laurent Gisel, "Grammar: Rules in a Cyber Conflict", in Patryk Pawlak and François Delerue (eds), *A Language of Power? Cyber Defence in the European Union*, Chaillot Paper, EUISS, Paris, 2022, pp. 65–67. For an up-to-date overview of State positions on the matter, see "Attack (International Humanitarian Law)", *Cyber Law Toolkit*, 30 March 2023, available at: https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).

27 ICRC Commentary on the APs, above note 13, pp. 618–619; see also Supreme Court of Israel, *Public Committee against Torture*, above note 12, para. 33.

28 ICRC Interpretive Guidance, above note 15, p. 48; see also Nils Melzer, *Summary Report of the Third Expert Meeting on the Notion of Direct Participation in Hostilities*, ICRC, Geneva, 23–25 October 2005 (2005 DPH Report), pp. 29 (wiretapping), 31 (clearing mines).

29 Tallinn Manual 2.0, above note 22, Rule 97, para. 5.

30 See e.g. Ryan Gallagher, "'Cyber Partisans' Say They Hacked Belarus Rail to Disrupt Russian Troops", *Bloomberg*, 24 January 2022, available at: www.bloomberg.com/news/articles/2022-01-24/hackers-say-they-breached-belarusian-rail-to-stop-russian-troops.

31 ICRC Interpretive Guidance, above note 15, p. 50.

32 Nils Melzer, *Summary Report of the Second Expert Meeting on the Notion of Direct Participation in Hostilities*, ICRC, Geneva, 25–26 October 2004 (2004 DPH Report), p. 5.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

sufficient to meet the "threshold of harm" criterion.[33] This question is closely related to the issue of direct causation, which will be analyzed in the next section.

Finally, with respect to scenario 3, the majority of activities taken by private companies will fall well below the threshold of harm. This includes activities with some relevance to national cyber defence or to the prosecution of the war effort, such as the development of generic cyber capabilities designed for military use, training military cyber personnel, hardening existing cyber defences, or strengthening societal cyber resilience in anticipation of enemy military operations. All of these are types of "conduct that merely builds up or maintains the capacity of a party to harm its adversary".[34] As such, they are excluded from the notion of direct participation in hostilities.[35] Conversely, some forms of action taken by private companies to defend the domestic cyber infrastructure against the enemy's military cyber operations may impede or thwart such operations, and thus potentially cross the required threshold of harm.[36] This would be the case if the company conducted a "hack-back" against the source of the enemy operation – but not if it was merely restoring its system after that operation had ended.

Direct causation

The second criterion, that of direct causation, has been described as "really the key principle in this area",[37] and this is arguably also the case for our present purposes. The existence of a direct causal link may be established more easily in some of the examples discussed here than in others, however. The ICRC Interpretive Guidance explains that according to the criterion, the harm must be brought about in "one causal step".[38] Launching an offensive cyber operation (scenario 1) or a hack-

33 ICRC Interpretive Guidance, above note 15, p. 48 fn. 103.

34 *Ibid.*, p. 53.

35 But see Tallinn Manual 2.0, above note 22, Rule 97, para. 5, describing a minority position according to which "maintaining passive cyber defences of military cyber assets" also qualifies as direct participation in hostilities, because by enhancing one State's own military capacity, it necessarily weakens an adversary's relative position. In the view of the present author, this is an overbroad reading which is inconsistent with generally accepted interpretations of IHL in this context: for instance, it is generally accepted that civilians working in munitions factories in rear areas are not directly participating in hostilities even though this activity does enhance the military capacity of their State. See e.g. Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, The Hague, 1982, p. 344; ICRC Interpretive Guidance, above note 15, p. 53 fn. 123; DoD Military Manual, above note 17, para. 5.8.2.2 fn. 255.

36 See also Jonathan Horowitz, "Private Companies in Cyber Operations during Armed Conflict", *Articles of War*, 13 January 2022, available at: https://lieber.westpoint.edu/private-companies-cyber-operations-armed-conflict/.

37 D. Akande, above note 23, p. 187.

38 ICRC Interpretive Guidance, above note 15, p. 53; but see e.g. Michael N. Schmitt, "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis", *Harvard National Security Journal*, Vol. 1, 2010, p. 30 ("[t]he reference to 'one causal step' is unfortunate"); David Wallace, Shane Reeves and Trent Powell, "Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines", *Harvard National Security Journal*, Vol. 12, 2021, p. 194 (arguing that "the 'case-by-case' or 'contextual' approach taken by the United States and others is arguably more

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

back (scenario 3) against the enemy is less difficult to classify in this regard: the requisite harm may be reasonably expected to result directly from the act in question.[39] This is irrespective of the geographic or temporal distance between the civilian's action and the relevant harm: what matters is causal proximity, not geographic or temporal proximity.[40]

By contrast, providing intelligence on enemy movements through a smartphone app (scenario 2) is less causally proximate. Whether this provision of information by individual civilians results in the requisite harm depends on the action of the receiving party to the conflict, and for the criterion to be fulfilled, the provision of information must be an integral part of a coordinated operation directly causing the harm.[41] A lot turns on the specific circumstances of each case. As noted earlier, in the kinetic context, there is "general agreement that civilians merely answering questions asked by passing military personnel could not be considered as directly participating in hostilities".[42] Similarly, answering a general question through an app, even if the answer could be of military value to a belligerent, would normally be too remote to qualify as directly causing the requisite harm.[43] As long as the military information being gathered and shared by civilians is of a general nature, the act of gathering and sharing the information does not constitute direct participation in hostilities.[44]

The reverse would only be the case in the exceptional circumstances in which the information in question was provided "with a view to the execution of a specific hostile act".[45] This is a long-standing interpretation, as evidenced by the 1923 Hague Rules of Air Warfare, according to which "[t]he term 'hostilities' includes the transmission … of military information *for the immediate use of a belligerent*".[46] An example in our present context would be the provision of exact targeting coordinates for a specific military objective, as an integral part of a concrete and coordinated tactical operation by the belligerent in question to

operationally palatable as it provides the necessary flexibility for determining whether a particular cyber operation would amount to a direct participation in hostilities").

39 See Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 6, describing "conducting DDoS operations against enemy military external systems" as an "unambiguous example" of direct participation in hostilities.

40 ICRC Interpretive Guidance, above note 15, p. 55. See also 2005 DPH Report, above note 28, p. 35; D. Wallace, S. Reeves and T. Powell, above note 38, p. 180.

41 ICRC Interpretive Guidance, above note 15, pp. 54–55.

42 2004 DPH Report, above note 32, p. 5.

43 But see Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 5, describing "gathering information on enemy operations by cyber means and passing it to one's own State's armed forces" as an "unambiguous example" of direct participation in hostilities. For reasons described in the main text, it is submitted that this is an overbroad interpretation of the relevant law.

44 Shane Darcy, *To Serve the Enemy: Informers, Collaborators, and the Laws of Armed Conflict*, Oxford University Press, Oxford, 2019, p. 113.

45 ICRC Interpretive Guidance, above note 15, p. 66.

46 Hague Rules of Air Warfare, 1923, Article 16, emphasis added. More recently, this interpretation has been embraced by the ICTY and the ICC: ICTY, *The Prosecutor v. Pavle Strugar*, Case No. IT-01-42-A, Judgement (Appeals Chamber), 17 July 2008, para. 177; ICC, *The Prosecutor v. Bahr Idriss Abu Garda*, Case No. ICC-02/05-02/09, Decision on the Confirmation of Charges, 8 February 2010, para. 81.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

attack that target.[47] The requirement that the intelligence must be gathered and transmitted *for the purposes of a specific attack* is also echoed in the positions of the few States that have expressed their views on these matters in the digital context.[48]

This difference may be subtle, but it is critically important. There is a wide range of situations in which reporting the position of the enemy to the authorities is a normal (i.e., non-hostile) civilian conduct that should not be construed as an act leading to the person's targetability.[49] Otherwise, for instance, internally displaced persons arriving in camps would not be able to tell their stories to the government authorities if those stories contained information on the location of enemy forces – or a civilian air traffic controller could not report the approach of enemy military aircraft in the course of her work – without becoming targetable under IHL.[50] Such interpretations would lead to a manifestly absurd result that would be impossible to reconcile with the protective object and purpose of the relevant rules on the conduct of hostilities.[51]

Belligerent nexus

Determining whether the belligerent nexus criterion is met may again be more straightforward in some of the above examples than in others. The act of launching an offensive cyber operation at the instigation of one's own State against that State's enemy during an armed conflict (scenario 1) is a type of action specifically designed to support the actor's own State and to be detrimental to the other. Ordinarily, such forms of conduct will suffice to meet the criterion.

Things are less clear with regard to the transmission of intelligence on enemy movement (scenario 2). As with the direct causation criterion, a lot will depend on the exact parameters of the app and the type of information provided. Informing one party to the conflict about the military actions of the other may be specifically designed to support one to the detriment of another, thus fulfilling the belligerent nexus criterion. However, doing so may also be designed to enable

47 See ICRC Interpretive Guidance, above note 15, pp. 54–55. See also 2005 DPH Report, above note 28, p. 22 ("only intelligence gathering that had a direct connection to attack or defence should be regarded as part of the hostilities"); 2004 DPH Report, above note 32, p. 5 ("the provision of information with the intent to influence the hostilities should constitute DPH").

48 French Position Paper, above note 20, p. 15 ("the penetration of a military system by a party to an armed conflict with a view to gathering tactical intelligence for the benefit of an adversary *for the purposes of an attack* constitutes direct participation in hostilities") (emphasis added); German Position Paper, above note 21, p. 8 ("transmitting tactical targeting information *for an attack* … could suffice in order to consider a civilian person as directly participating in hostilities") (emphasis added).

49 See also ICRC Commentary on the APs, above note 13, p. 901, para. 3187, noting that "gathering and transmission of military information" *per se* are examples of "*indirect* acts of participation" in hostilities (emphasis added).

50 I am grateful to Ramin Mahnad for suggesting these examples.

51 For an analysis of the object and purpose of these rules from the perspective of cyber operations during armed conflicts, see Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, Vol. 48, No. 1, 2015, pp. 77–78 (with references), available at: https://tinyurl.com/2emrppjj.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

civilian warning and evacuation, to support the work of civil defence organizations, or to achieve other non-belligerent purposes, in which case the criterion would not be met.[52] Furthermore, if the questions and answers transmitted through an app are so general that the civilians involved "are totally unaware of the role they are playing in the conduct of hostilities", then the action of transmitting the information would not reach the nexus threshold.[53] To say otherwise would mean removing the protection against attack from individuals who are being wholly instrumentalized and who therefore cannot be regarded as performing a legally relevant action.[54]

The belligerent nexus criterion is even harder to meet with respect to the conduct of private companies (scenario 3). It could be argued that when such companies engage in acts of cyber defence, even if mandated by the law, they do so primarily in order to protect their own interests (such as limiting exposure to liability, protecting their share value or simply maintaining their reputation) rather than to support the war effort of one State and/or to harm another.

This raises the question of the relevance of subjective intent in evaluating the belligerent nexus criterion. The ICRC Interpretive Guidance bases its approach strictly on the objective purpose of the act in question, noting that "the subjective motives driving a civilian to carry out a specific act cannot be reliably determined during the conduct of military operations and, therefore, cannot serve as a clear and operable criterion for 'split second' targeting decisions".[55] With some narrow exceptions,[56] whether or not a person becomes targetable under IHL is contingent on the objective nature of their conduct, and not on their inner state of mind.[57]

52 See, similarly, Michael N. Schmitt, "Ukraine Symposium – Using Cellphones to Gather and Transmit Military Information, A Postscript", *Articles of War*, 4 November 2022, section "Warning the Civilian Population", available at: https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/.

53 ICRC Interpretive Guidance, above note 15, p. 60. See also e.g. Byron Tau, "App Taps Unwitting Users Abroad to Gather Open-Source Intelligence", *Wall Street Journal*, 24 June 2021, available at: www.wsj.com/articles/app-taps-unwitting-users-abroad-to-gather-open-source-intelligence-11624544026 (reporting on how innocuous data collected through apps can be used for military purposes).

54 ICRC Interpretive Guidance, above note 15, p. 60.

55 *Ibid.*, p. 59 fn. 150.

56 Such as when a civilian is "totally unaware" of the fact that they are involved in the conduct of hostilities: see note 53 above and the associated text. See also J. Horowitz, above note 7, discussing the relevance of subjective considerations in the context of technological companies operating in armed conflict environments.

57 See e.g. Germany, Federal Prosecutor General at the Federal Court of Justice (Bundesgeneralanwalt beim Bundesgerichtshof), *Investigation Proceedings against Colonel (Oberst) Klein and Company Sergeant Major (Hauptfeldwebel) Wilhelm Because of Suspected Offences under the International Crimes Code and Other Offences*, Case No. 3 BJs 6/10-4, Decision to Terminate Proceedings Pursuant to Section 170 Para. 2 Sentence 1 of the Penal Procedure Code, 16 April 2010 (so-called *Fuel Tankers* case), p. 60: "Die unmittelbare Teilnahme an Feindseligkeiten im Sinne des Konfliktsvölkerrechts ist von der Willensrichtung des sich Beteiligenden unabhängig, denn der zeitweilige Verlust des Schutzes als Zivilist ist eine Folge davon, dass diese Person objektiv eine militärische Bedrohung darstellt." (ICRC translation: "The direct participation in hostilities as understood under the international law of armed conflict is independent of the individual will of the person concerned because the temporary loss of protection as a civilian is the consequence of the person objectively constituting a military threat.") However, some States incorporate the element of intent into their assessment of whether an act

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

It is submitted that the same approach should apply to the involvement of private companies in national cyber defence. The adversary will normally not be able to determine the subjective motives of the acting entity, and it would be particularly unrealistic to saddle it with this burden in the cyber context, which is characterized by geographical remoteness and uncertain attribution.[58] Therefore, the objective purpose should be determined by reference to the design of the operation in question.[59] If the operation can reasonably be regarded as being designed to support one party to the conflict to the detriment of another, it would thus meet the nexus criterion irrespective of the associated subjective motivations.[60] If not (for example, because a company's operations affect both parties equally), then the criterion would not be met. This may of course be difficult to determine in practice;[61] in case of doubt, the conduct should be presumed not to qualify as direct participation in hostilities.[62]

Additionally, if the operation is objectively taken in defence of the company or its infrastructure, it could potentially fall within the separate exemption of "individual self-defence" against unlawful acts of violence.[63] As noted in the ICRC Interpretive Guidance, "although the use of force by civilians to defend themselves against unlawful attack or looting, rape, and murder by marauding soldiers may cause the required threshold of harm, its purpose clearly is not to support a party to the conflict against another".[64] Similarly, protecting one's own networks against existing or imminent unlawful cyber harm is conduct not designed to support any party to a conflict and as such would lack belligerent nexus.[65]

constitutes direct participation in hostilities: see e.g. Danish Military Manual, above note 19, p. 171; Norwegian Military Manual, above note 17, paras 3.24, 3.27.

58 Cf. Florian J. Egloff and Myriam Dunn Cavelty, "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics", *Journal of Cybersecurity*, Vol. 7, No. 1, 2021, p. 5, explaining that the attacker's intent is an element of attribution that is frequently difficult to substantiate with robust data.

59 ICRC Interpretive Guidance, above note 15, p. 59.

60 See *ibid.*, pp. 63–64, describing the decisive question as "whether the conduct of a civilian, in conjunction with the circumstances prevailing at the relevant time and place, can reasonably be perceived as an act designed to support one party to the conflict by directly causing the required threshold of harm to another party".

61 See J. Horowitz, above note 7.

62 ICRC Interpretive Guidance, above note 15, pp. 75–76; see also e.g. New Zealand Military Manual, above note 17, p. 6-15, para. 6.5.11. But see Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 13, noting that the "International Group of Experts was divided over the issue of whether a presumption against direct participation applies"; and D. Wallace, S. Reeves and T. Powell, above note 38, p. 196, asserting that it is "unclear" how this dilemma will be resolved in the future.

63 The use of force by individuals in defence of themselves or others should be distinguished from the use of force by States in self-defence against an armed attack, which is governed by the *jus ad bellum* and is beyond the scope of this article. See, similarly, ICRC Interpretive Guidance, above note 15, p. 61 fn. 158.

64 *Ibid.*, p. 61. See also ICRC, *Summary Report of the First Expert Seminar on Direct Participation in Hostilities under International Humanitarian Law*, Geneva, September 2003 (2003 DPH Report), p. 6: "All the experts who spoke on the subject stressed that individual civilians using a proportionate amount of force in response to an unlawful and imminent attack against themselves or their property should not be considered as directly participating in hostilities."

65 See, further, J. Horowitz, above note 7, arguing that it is in companies' interest to explain their actions in order to mitigate risks.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Interim conclusion

Only if a certain form of civilian involvement meets all three of these criteria simultaneously will the conduct in question qualify as direct participation in hostilities. The foregoing analysis demonstrates that this outcome is an exception rather than the rule. While certain offensive cyber operations conducted by civilians (scenario 1) may in some circumstances qualify as direct participation in hostilities, most forms of provision of information by civilians through smartphone apps (scenario 2) and cyber defence activities by private companies (scenario 3) do not.

Nonetheless, the exceptions cannot be ignored, and their legal consequences need to be understood. In addition, the narrow conclusions endorsed here may be challenged by others who interpret the applicable criteria more extensively than the present article, with the result that more types of conduct would be perceived as direct participation. This only underlines the need to understand the legal implications of such qualifications, both for the individuals and for the States concerned. This is what we turn to in the remaining two sections of this article.

Legal implications for individuals

Violation of international or domestic law?

To begin with, it might be queried whether the forms of engagement described above are unlawful for the individuals concerned: do civilians violate IHL by directly participating in hostilities? In this regard, it is noteworthy that IHL provides only combatants with an express right to participate directly in hostilities.[66] According to one view (expressed succinctly by the British military lawyer General A. P. V. Rogers), "[t]he inference is that others do not have the right to participate directly in hostilities and, *if they do, they violate the law of war*".[67] A similar (and similarly rare) position can be found in a 1976 US Air Force pamphlet, according to which there is an "*obligation* on the part of civilians not to take a direct part in hostilities".[68]

66 See Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 43(2).

67 Anthony Rogers, "Combatant Status", in Elizabeth Wilmshurst and Susan Breau (eds), *Perspectives on the ICRC Study on Customary International Humanitarian Law*, Cambridge University Press, Cambridge, 2007, p. 122.

68 United States, "International Law – The Conduct of Armed Conflict and Air Operations", Air Force Pamphlet 110-31, Department of the Air Force, 19 November 1976, p. 5-8. Air Force Pamphlet 110-31 infers this obligation from the general immunity from attack owed to civilians under IHL. Another historical example can be found in United Kingdom, *The Law of War on Land, Being Part III of the Manual of Military Law*, Her Majesty's Stationery Office, London, 1958, p. 626 (no longer in force). See also Swiss Military Manual, above note 17, para. 172: "Les personnes civiles ne peuvent pas participer aux hostilités." (ICRC translation: "Civilians may not participate in hostilities.")

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

This interpretation is not generally accepted, however. The dominant position – also shared by the ICRC – is that "IHL neither prohibits nor privileges civilian direct participation in hostilities".[69] Probably the only treaty prohibition against involving civilians in armed conflict is the prohibition against privateering found in the 1856 Paris Declaration on maritime law,[70] which is of little relevance in the context discussed in this article. Therefore, while it is certainly true that civilians "were never meant to directly participate in hostilities on behalf of a party to the conflict",[71] there is no express prohibition against them doing so. It logically follows that civilian direct participation in hostilities does not, in and of itself, constitute a war crime.[72] This is confirmed by the fact that none of the statutes of past or existing international criminal tribunals have criminalized such conduct.[73] Returning to the cyber context, the Tallinn Manual 2.0 group of experts also observed that IHL "does not bar any category of person from participating in cyber operations".[74]

By contrast, acts of direct participation in hostilities are often criminalized under domestic law, together with numerous other forms of harmful behaviour that may fall below the direct participation threshold as far as IHL is concerned. Domestic statutes may do so expressly, or they may provide for offences that cover the same forms of behaviour as those typically committed by individuals engaged in armed conflicts: deliberate killing or injuring of another, damaging or destroying property, or – more relevant in the present context – computer-related offences such as the creation, use or distribution of malicious software.[75] Because civilians are by definition not combatants, they are not shielded from domestic prosecution for such acts by combatant immunity.[76] Similarly, if captured, civilians who have directly participated in hostilities are not entitled to prisoner-of-war status.[77]

69 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, 2011, p. 44.

70 Declaration Respecting Maritime Law, Paris, 1856, Art. 1 ("Privateering is, and remains, abolished").

71 ICRC Interpretive Guidance, above note 15, pp. 38–39.

72 Nils Melzer, "Direct Participation in Hostilities", in Dražan Djukić and Niccolò Pons (eds), *The Companion to International Humanitarian Law*, Brill, Leiden, 2018, p. 300. See also 2003 DPH Report, above note 64, p. 9 ("No one contested that direct participation in hostilities by a civilian could not be considered a war crime"); Michael N. Schmitt, "Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees", *Chicago Journal of International Law*, Vol. 5, 2005, pp. 520–521 (arguing that while mere direct participation, without more, is not a war crime, the acts underlying direct participation may be punishable).

73 See ICRC Interpretive Guidance, above note 15, p. 84 fn. 226 (with references). Reportedly, the drafters of the 1998 Rome Statute of the ICC did not even consider any proposal to include direct participation in hostilities as a war crime in the Statute. See A. Rogers, above note 67, p. 122 fn. 100.

74 Tallinn Manual 2.0, above note 22, Rule 86.

75 For a comparative analysis of cyber crime offences criminalized by national laws around the world, see UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, February 2013, pp. 77–106, available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

76 M. Bothe, K. J. Partsch and W. A. Solf, above note 35, p. 278; ICRC Interpretive Guidance, above note 15, p. 84.

77 See e.g. Knut Ipsen, "Combatants and Non-Combatants", in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 4th ed., Oxford University Press, Oxford, 2021, p. 97.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Loss of protection from attack and the related safeguards

In addition, a key consequence of direct participation in hostilities is the loss of protection from attack for the individual concerned.[78] In this sense, there is no difference between "kinetic" and "cyber" direct participation in hostilities. In practical terms, the act of direct participation in hostilities by a civilian renders them liable to be attacked by any lawful means, whether cyber or not.[79]

However, the specific characteristics of the cyber environment, together with the remoteness implicit in practically any cyber activity, pose certain additional challenges as well as safeguards relevant to the targeting of individuals who have directly participated in hostilities through cyber or digital means.

First, there may be certain territorial considerations to be taken into account. Until now, a tacit assumption of this article has been that the individuals concerned are located in the territory of one of the parties to the conflict. However, it is certainly conceivable that civilians could engage from outside of those territories in cyber activities that would fall under the definition of direct participation in hostilities if IHL applied. If that is the case, other branches of international law – such as the law on the use of force, the law of neutrality, or human rights law – will contain important limitations that will in most cases preclude the application of lethal force against such individuals.[80]

Second, IHL imposes important temporal considerations. Civilians only lose protection from attack "for such time as" they directly participate in hostilities.[81] This means that if the specific act that constitutes direct participation ends, their protection against attack is restored.[82] The exact beginning and end of specific acts amounting to direct participation in hostilities must therefore be determined with utmost care.[83]

Consider, for example, a civilian using a smartphone app to provide tactical intelligence to attacking forces (scenario 2).[84] As noted earlier, in certain very narrow circumstances, such conduct may amount to direct participation in

78 ICRC Commentary on the APs, above note 13, p. 619, para. 1944; ICRC Interpretive Guidance, above note 15, p. 69; Program on Humanitarian Policy and Conflict Research, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Harvard University, 15 May 2009, *chapeau* to section F; Tallinn Manual 2.0, above note 22, Rule 91, commentary para. 1; UK Military Manual, above note 17, para. 5.3.2; DoD Military Manual, above note 17, para. 16.5.5.

79 Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 3.

80 See, generally, Michael Ramsden, "Targeted Killings and International Human Rights Law: The Case of Anwar Al-Awlaki", *Journal of Conflict and Security Law*, Vol. 16, No. 2, 2011; Jelena Pejic, "Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications", *International Review of the Red Cross*, Vol. 96, No. 893, 2014, especially pp. 70–75, 100–101. Discussing these areas of law is outside of the scope of the present article.

81 AP I, Art. 51(3); Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II), Art. 13(3); ICRC Customary Law Study, above note 12, Rule 6.

82 ICRC Interpretive Guidance, above note 15, p. 70.

83 *Ibid.*, p. 65.

84 For an analysis of the temporal element in the context of technology companies' involvement in armed conflicts (scenario 3), see J. Horowitz, above note 7.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

hostilities.[85] Importantly, the information thus provided (e.g. the targeting coordinates sent via a chat function in the app or an image of an enemy military objective uploaded through the app) may remain stored in the phone after such engagement. Does the act of direct participation continue while the information is available in the phone concerned?

It is submitted that such a reading would be overbroad, and that the civilian involvement ends at the moment when the information is provided. This is because at that point in time, the relevant conduct (i.e., the "act"[86]) of the civilian comes to an end, and the mere carrying of a phone containing militarily relevant information cannot be considered as direct participation,[87] even if the object as such may continue to have military value.[88] The individual's conduct does not present any danger for the adversary any more, and as such they may no longer be directly attacked.[89]

Third, there are uncertainty considerations that must be taken into account. In order to avoid the erroneous or arbitrary targeting of civilians, parties to a conflict must take all feasible precautions in verifying whether a person is a civilian and, if that is the case, whether they are directly participating in hostilities.[90] In case of doubt, the person in question must be presumed to be protected against direct attack.[91] As explained by Yoram Dinstein, this interpretation is necessary "to ensure that soldiers tasked with the mission of winnowing out false civilians who are *de facto* combatants will not treat innocent civilians as targetable, 'shooting first and asking questions later'".[92]

Fourth, even where a civilian loses protection from attack, any use of force against them remains governed by other rules of IHL. In particular, if attacking the individual may be expected to result in disproportionate incidental civilian harm[93]

85 See the above section on "Application of the General Rule to the Three Scenarios".

86 See also Tallinn Manual 2.0, above note 22, Rule 97, commentary para. 4: "In the cyber context, it is essential to emphasize that an 'act' is required by the individual concerned."

87 See also Supreme Court of Israel, *Public Committee against Torture*, above note 12, para. 39: "A civilian taking a direct part in hostilities one single time, or sporadically, who later detaches himself from that activity, is a civilian who, starting from the time he detaches himself from that activity, is entitled to protection from attack."

88 The device containing this information may continue to qualify as a military objective if fulfils the definition of military objective in the circumstances ruling at the time: see AP I, Art. 52(2). For example, if the information stored in the device was outdated or had otherwise lost its military value, the device would not qualify as a military objective as its destruction, capture or neutralization would no longer offer a "definite military advantage" as required by the law. See, further, ICRC Commentary on the APs, above note 13, p. 636, para. 2024.

89 See ICRC Commentary on the APs, above note 13, p. 1453, para. 4789, noting that protection is denied "for as long as [the individual's] participation lasts. Thereafter, as he no longer presents any danger for the adversary, he may not be attacked." See also M. Bothe, K. J. Partsch and W. A. Solf, above note 35, p. 342: "while participating directly in hostilities[, civilians] present an immediate threat to the adverse Party and, accordingly, they are subject to direct attack to the same extent as combatants".

90 AP I, Art. 57(2)(a)(i); ICRC Customary Law Study, above note 12, Rule 16.

91 See above note 62.

92 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 4th ed., Cambridge University Press, Cambridge, 2022, p. 206, quoting Frits Kalshoven, *Reflections on the Law of War: Collected Essays*, Cambridge University Press, Cambridge, 2007, pp. 73–74.

93 See AP I, Arts 51(5)(b), 57(2)(a)(iii); ICRC Customary Law Study, above note 12, Rule 14.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

or if it was feasible to obtain a similar military advantage while causing less or no incidental civilian harm, then the attack would be prohibited by IHL.[94] Moreover, IHL expressly provides that the presence of civilians directly participating in hostilities among the civilian population does not deprive the population at large of the protection from attack to which it is entitled.[95]

Finally, it is important to distinguish the lawfulness of an attack from its operational feasibility or military value. In practical terms, parties to armed conflicts may prefer to target the objects used by the civilian in question – such as the network, the device or the app – rather than the person. Doing so may be more militarily expedient and thus preferable as a matter of policy. (It would also have to be determined whether the said object qualifies as a military objective, and the operation against it would have to comply with all other applicable rules of IHL.[96]) However, the fact remains that civilians may indeed exceptionally lose their legal protection from attack through these forms of involvement. In the next section, we will analyze what this means from a systemic perspective.

Legal implications for States

International humanitarian law

The principle of distinction is one of the oldest principles in IHL and a cornerstone of that body of law. The International Court of Justice (ICJ) has described it as a "cardinal" and "intransgressible" principle that is part of "the fabric of humanitarian law".[97] It reflects the prevailing post-Westphalian philosophical and political paradigm according to which the monopoly on the legitimate use of force belongs to States.[98] As Jean-Jacques Rousseau wrote in *The Social Contract*, war is a relation "not between man and man, but between State and State".[99] In other words, civilians are not the enemies of States, and they must thus be spared, as far as possible, from the effects of any hostilities between States.[100]

This paradigm has also been reaffirmed by the international community in the cyber context. In particular, the UN General Assembly has repeatedly given

94 See AP I, Art. 57(3); ICRC Customary Law Study, above note 12, Rule 21.
95 AP I, Art. 50(3).
96 See also J. Horowitz, above note 7, endorsing the same policy preference while warning that cyber operations against military objectives that also provide services to civilians pose significant potential risks, in particular when they are detrimental to critical infrastructure that supports essential civilian services such as health care, electricity and water.
97 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, *ICJ Reports 1996* (Nuclear Weapons Advisory Opinion), para. 78.
98 Max Weber, *The Vocation Lectures*, Hackett, Indianapolis, IN, 2004, p. 33: "the state is the form of human community that … lays claim to the monopoly of legitimate violence within a particular territory".
99 Jean-Jacques Rousseau, *The Social Contract*, trans. G. D. H. Cole, Cosimo Classics, New York, 2008 (first published 1762), pp. 19–20.
100 See e.g. UNGA Res. 2444 (XXIII), 19 December 1968, para. 1(c): "distinction must be made at all times between persons taking part in the hostilities and members of the civilian population to the effect that the latter be spared as much as possible".

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

unanimous endorsement to the consensus reports issued by several Groups of Governmental Experts, which have described distinction as an "established international legal principle" applicable to the use of information and communications technologies by States.[101] The principle of distinction and the values it represents are today part of the irreducible core of the normative framework applicable during armed conflicts, including when these involve new means and methods of warfare.[102]

In this respect, encouraging civilian participation in cyber activities that may amount to direct participation in hostilities raises several crucial systemic-level concerns. One has to begin with the humanitarian concern: such acts of encouragement undermine the central humanitarian value that undergirds the principle of distinction, namely the protection of those who must be spared from the effects of armed conflict.

In modern-day armed conflicts, civilians are killed and injured at much higher rates than their combatant counterparts.[103] Any pattern of conduct which makes them more susceptible to harm is thus by definition morally suspect and practically problematic. As Eric Jensen has noted, in the kinetic context, encouraging individuals "to fight as civilians will inevitably lead to more civilian casualties as combatants struggle to distinguish the fighters amongst the civilians".[104] The same concern arises in the cyber context.

An objection could be made that the kinetic targeting of individuals based on their cyber participation in hostilities is unlikely. For example, in 2019, France's Ministry of Armies noted in a public position paper that "[g]iven the difficulties of identifying the perpetrators of a cyberattack, the targeting of such individuals remains marginal".[105] However, technical attribution capabilities have dramatically improved in the recent period,[106] so over time, the risk exists that such targeting may become less marginal.

In addition, there have already been reports of militaries targeting civilians in combat zones for being suspected of using their mobile phones to report the enemy's location.[107] If parties to armed conflicts encourage civilians to engage in

101 *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, 14 July 2021; UNGA Res. 76/19, 8 December 2021, para. 2; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, para. 28(d); UNGA Res. 73/27, 11 December 2018, para. 1.

102 ICRC, "Principles of IHL (Distinction, Proportionality) Have Direct Bearing on Cyber Operations", Statement to the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 12 February 2020, available at: www.icrc.org/en/document/principles-international-humanitarian-law-distinction-proportionality-have-direct-bearing.

103 See e.g. Frederick M. Burkle, "Revisiting the Battle of Solferino: The Worsening Plight of Civilian Casualties in War and Conflict", *Disaster Medicine and Public Health Preparedness*, Vol. 13, No. 5–6, 2019, p. 838.

104 Eric Talbot Jensen, "Applying a Sovereign Agency Theory of the Law of Armed Conflict", *Chinese Journal of International Law*, Vol. 12, 2012, p. 701 fn. 74.

105 French Position Paper, above note 20, p. 15.

106 See e.g. Kristen E. Eichensehr, "The Law and Politics of Cyberattack Attribution", *UCLA Law Review*, Vol. 67, 2020, p. 529.

107 See e.g. Dan Bilefsky, "A Ukrainian Appeals Court Reduces the Life Sentence of a Russian Soldier Tried for War Crimes", *New York Times*, 29 July 2022.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

this type of conduct, such incidents may become much more common, including in situations where the civilian in question was using the phone for another reason – for instance, to warn their families to leave or to seek shelter.

This humanitarian concern translates into legal concerns under IHL. To begin with, there is a strong strand of scholarship arguing that the practice of involving civilians in combat functions is eroding (or undermining) the principle of distinction.[108] As noted, this principle requires that – insofar as persons are concerned – parties to armed conflicts must at all times distinguish between civilians and combatants.[109] The principle is most effective in practice if participation in hostilities is limited to those endowed with combatant privilege.[110] In other words, blurring the distinction between combatants and civilians by definition "endanger[s] the protection afforded to the latter".[111] This is because if the lines become unclear, then there is a risk that parties to armed conflicts may gradually begin to err on the side of considering all individuals in the enemy population to be involved in hostile acts, thus diminishing restraints on attacks against them.[112]

For some authors, the deliberate contribution to such risks by States does not merely "erode" or "undermine" the principle of distinction, but constitutes a standalone violation of IHL attributable to the State in question. In particular, Lindsey Cameron and Vincent Chetail write:

> Respect for the principle of distinction entails that *a state may not use civilians to directly participate in hostilities*. Indeed, if a state were to do so, it would be putting its own civilians in jeopardy since civilians directly participating in hostilities lose protection against attack and may be arrested and tried for such acts. What is more, states are responsible for ensuring that the principle of distinction is upheld. If a state were to permit civilians to undertake combat functions, or to require them by contract to do so, *that state would violate its obligation to uphold the principle of distinction*.[113]

108 See e.g. Gabor Rona, "When Considering CIA Targeted Killings, Don't Forget International Law!", *Just Security*, 5 April 2016, available at: www.justsecurity.org/30426/cia-targeted-killings-dont-forget-international-law/ ("blurring the lines between combatant and civilian – as occurs when the CIA directly participates in hostilities – creates a precedent that undermines the principle of distinction, even if that participation is not unlawful"); Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Edward Elgar, Cheltenham, 2019, p. 25 ("the increasing civilianization of armed forces is … eroding the principle of distinction because individuals outside of the armed forces are increasingly performing several functions that contribute not only to a State's military capacity but even directly to battlefield action"); D. Wallace, S. Reeves and T. Powell, above note 38, p. 174 ("civilian involvement in armed conflicts … undermines the [law of armed conflict's] core principle of distinction").

109 AP I, Art. 48; ICRC Customary Law Study, above note 12, Rule 1.

110 K. Mačák, above note 8, p. 421.

111 Giulio Bartolini, "The Participation of Civilians in Hostilities", in Michael John Matheson and Djamchid Momtaz (eds), *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts*, Martinus Nijhoff, Leiden, 2010, p. 325.

112 *Ibid.*, p. 357.

113 Lindsey Cameron and Vincent Chetail, *Privatizing War*, Cambridge University Press, Cambridge, 2013, p. 104 (emphasis added).

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

This is a powerful argument that goes a long way towards addressing the protective needs identified in this article. However, it may be challenging to identify a precise legal basis for such a generalized obligation to uphold the principle of distinction, or to determine the exact contours of this obligation. Even Article 48 of AP I – sometimes described as "the basic rule of distinction"[114] – is narrower in its remit: it demands that the parties to the conflict should distinguish between the civilian population and combatants at all times, but it does not establish a generalized obligation to uphold the principle that underpins the text of the rule. In this author's view, it is thus preferable to examine specific IHL obligations that flow from the principle of distinction. Three of them stand out in this context: the obligation of constant care, the obligation to take passive precautions, and the obligations relating to participation in hostilities by children.

First, parties to armed conflicts are bound by the obligation of constant care, which mandates that in the conduct of military operations, constant care must be taken to spare the civilian population, civilians and civilian objects.[115] Several States – including France[116] and Germany[117] – have explicitly stated that this obligation also applies in the context of cyber operations, and this view is also shared by the ICRC.[118] In the Tallinn Manual process, it was agreed that this duty "requires commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon".[119] Exposing civilians to a loss of their protection under IHL is hardly compatible with the duty to spare them from such effects, as required by the constant care obligation.

Second, parties to armed conflicts are obliged to take, "to the maximum extent feasible", the necessary precautions "to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations".[120] Again, there is little doubt that this rule applies in the cyber context, and this has been expressly recognized by France.[121] In the Tallinn Manual context, it was underlined that this rule was "designed to

114 ICRC Commentary on the APs, above note 13, p. 598, para. 1863: "The basic rule of protection and distinction is confirmed in this article."
115 AP I, Art. 57(1); ICRC Customary Law Study, above note 12, Rule 15.
116 French Position Paper, above note 20, p. 15.
117 German Position Paper, above note 21, p. 9.
118 ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, ICRC Position Paper, Geneva, November 2019, p. 6, available at: www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.
119 Tallinn Manual 2.0, above note 22, Rule 114, commentary para. 4. Similarly, see Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects Of Cyber Operations during Armed Conflicts", *International Review of the Red Cross*, Vol. 102, No. 913, 2020, p. 324: "This obligation requires all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible, and to seek to avoid any unnecessary effects."
120 AP I, Art. 58(c).
121 French Position Paper, above note 20, p. 16.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

protect against death or injury to civilians".[122] Therefore, encouraging civilians to directly participate in cyber hostilities, and thereby exposing them to the risk of losing their IHL protections, is in direct tension with this rule as well.

It could be objected that the constant care and passive precaution obligations are inapplicable to civilians who are directly participating in hostilities given that these individuals are no longer covered by the protection against attack normally afforded to civilians. However, that would be a misunderstanding of the present argument. This author accepts that for such time as civilians are engaged in an act of direct participation in hostilities, the protective ambit of these rules is removed from them.[123] However, that is not the case *before* they do so. It is submitted that until such time, parties remain bound by the said obligations, and encouraging civilians to cross the line, so to speak, towards unprotected territory is hard to reconcile with those obligations.[124]

Lastly, parties to armed conflicts must do everything feasible to ensure that children under 15 years of age do not directly participate in hostilities.[125] As noted in the ICRC Commentary on the relevant provision in AP I, "[t]he intention of the drafters of the article was clearly to keep children under fifteen outside armed conflict".[126] The age limit rises to 18 for States party to the African Charter on the Rights and Welfare of the Child,[127] and the ICRC recommends that all States adopt this higher age limit of 18.[128] Given that some of the activities on the digital battlefield may qualify as direct participation, this means that belligerents have an additional duty to prevent children under 15 or 18 from joining in. This is a pressing concern in view of the low threshold for digital forms of involvement discussed earlier[129] – not to mention the possibility that some of the relevant digital tools may be especially appealing to children, who are generally

122 Tallinn Manual 2.0, above note 22, Rule 121, commentary para. 9.

123 See e.g. Inter-American Commission on Human Rights, *Third Report on Human Rights Situation in Colombia*, OEA/Ser.L/V/II.102, Doc. 9, Rev. 1, 26 February 1999, para. 54 ("by virtue of their hostile acts, such civilians lose the benefits pertaining to peaceable civilians of precautions in attack and against the effects of indiscriminate or disproportionate attacks"); Supreme Court of Israel, *Public Committee against Torture*, above note 12, para. 46 (holding that the proportionality requirements do not cover the harm "to a civilian taking a direct part in the hostilities at such time as the harm is caused").

124 See also the text at above notes 103–112, noting that such practices increase the risk for other, protected civilians of being incidentally harmed or erroneously targeted.

125 AP I, Art. 77(2); AP II, Art. 4(3)(c); ICRC Customary Law Study, above note 12, Rule 137; Convention on the Rights of the Child, 1577 UNTS 3, 20 November 1989 (entered into force 2 September 1990), Art. 38 (2). Under the 1998 Rome Statute of the ICC, using children to "participate actively in hostilities" constitutes a war crime in both international and non-international armed conflicts. Rome Statute of the International Criminal Court, UN Doc. A/CONF.183/9, 17 July 1998 (entered into force 1 July 2002), Arts 8(2)(b)(xxvi), 8(2)(e)(vii).

126 ICRC Commentary on the APs, above note 13, p. 901, para. 3187.

127 African Charter on the Rights and Welfare of the Child, July 1990 (entered into force 29 November 1999), Art. 22(2). Article 2 of the Charter states that "[f]or the purposes of this Charter, a child means every human being below the age of 18 years".

128 Resolution 2 of the 26th International Conference of the Red Cross and Red Crescent in 1995 recommended that parties to conflict "take every feasible step to ensure that children under the age of 18 years do not take part in hostilities".

129 See the above section entitled "From General Trends to Qualitative and Quantitative Shifts in the Digital Space".

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

less able to accurately assess risk and may perceive such tools as just another game on their smart device.[130] Depending on the circumstances, specific examples of feasible measures could include implementing age restrictions and blocks on access to those digital tools the use of which may constitute direct participation in hostilities.[131] By contrast, failure to take any such measures could result in a standalone violation of the relevant IHL rules on the protection of children.

International human rights law

Encouragement of civilians to directly participate in hostilities during armed conflicts also raises concerns under international human rights law (IHRL). True, it is sometimes said that IHRL was designed for the environment of a normal State in the condition of peace.[132] However, it is now generally accepted that IHRL applies both in time of peace and during armed conflict.[133] This has been confirmed in a consistent line of case law of the ICJ;[134] it is also the view of most States[135] – Israel being one exception[136] – as well as of the International Law Commission[137] and various human rights mechanisms.[138]

There is a separate controversy as to the extent to which IHRL applies to extraterritorial conduct of States. However, that controversy does not arise here – at least not in relation to the practical scenarios considered in this

130 See Pontus Winther, "Military Influence Operations and IHL: Implications of New Technologies", *Humanitarian Law and Policy Blog*, 27 October 2017, available at: https://blogs.icrc.org/law-and-policy/2017/10/27/military-influence-operations-ihl-implications-new-technologies/.

131 Guidance is available regarding the adoption of measures that provide for age-appropriate child safety in digital applications. See e.g. International Telecommunication Union, *Guidelines for Policy-Makers on Child Online Protection*, Geneva, 2020, p. 44 on tools, services and settings.

132 See e.g. Christopher Greenwood, "Human Rights and Humanitarian Law – Conflict or Convergence?", *Case Western Reserve Journal of International Law*, Vol. 43, No. 1–2, 2010, p. 495.

133 See Kubo Mačák, "The Role of International Human Rights Law in the Interpretation of the Fourth Geneva Convention", *Israel Yearbook on Human Rights*, Vol. 52, 2022, p. 223.

134 See e.g. Nuclear Weapons Advisory Opinion, above note 97, para. 25; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, *ICJ Reports 2004*, para. 106; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, 19 December 2005, *ICJ Reports 2005*, paras 215–220.

135 See e.g. Helen Duffy, "Trials and Tribulations: Co-Applicability of IHL and Human Rights in an Age of Adjudication", in Ziv Bohrer, Janina Dill and Helen Duffy (eds), *Law Applicable to Armed Conflict*, Cambridge University Press, Cambridge, 2020, p. 39.

136 See e.g. Israel, "Comments from the State of Israel on the International Law Commission's *Draft Principles on the Protection of the Environment in Relation to Armed Conflicts* as Adopted by the Commission in 2019 on First Reading", 2020, para. 9.

137 ILC, *Draft Articles on the Effects of Armed Conflicts on Treaties*, 2011, reprinted in *Yearbook of the International Law Commission*, Vol. 2, Part 2, 2011, pp. 126–127, paras 49–50.

138 See e.g. Human Rights Committee, General Comment No. 31, "Nature of the General Legal Obligation on States Parties to the Covenant", UN Doc. CCPR/C/21/Rev.1/Add. 13, 26 May 2004, para. 11; Human Rights Committee, General Comment No. 35, "Article 9: Liberty and Security of Person", UN Doc. CCPR/C/GC/35, 16 December 2014, para. 64; Human Rights Committee, General Comment No. 36, "Article 6: Right to Life", UN Doc. CCPR/C/GC/36, 3 September 2019 (General Comment 36), para. 64; Committee on Economic, Social and Cultural Rights, "Concluding Observations: Israel", UN Doc. E/C.12/1/Add.90, 26 June 2003, para. 31; Committee against Torture, General Comment No. 2, "Implementation of Article 2 by States Parties", UN Doc. CAT/C/GC/2, 24 January 2008, para. 5; Committee on the Elimination of Discrimination against Women, "General Recommendation No. 28 on the Core Obligations of States parties under Article 2 of the Convention on the Elimination of All Forms of Discrimination against Women", UN Doc. CEDAW/C/GC/28, 16 December 2010, para. 11.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

article – given that our focus is on a State's conduct vis-à-vis the civilians who find themselves in that State's *own territory*, not abroad. On the basis of the foregoing, it can thus be inferred that IHRL is relevant when considering these forms of conduct in spite of the ongoing armed conflict; what remains to be determined is whether the conduct examined here is compatible with States' IHRL obligations.

It should be recalled that involving civilians in acts of direct participation in hostilities exposes them to the loss of protection against attack under IHL.[139] In other words, in doing so, the acting State exposes these individuals under its jurisdiction to the risk of grave injury or loss of life. At the same time, it is well established that the exposure of an individual to the risk of an effect that is proscribed by law – such as ill-treatment, torture or death – can amount to a violation of the concomitant right. For example, in the 2005 *Mamatkulov and Askarov v. Turkey* case, the European Court of Human Rights (ECtHR) held:

> It is the settled case-law of the Court that extradition by a Contracting State may give rise to an issue under Article 3 [of the European Convention on Human Rights, on prohibition of torture and inhuman or degrading treatment or punishment], and hence engage the responsibility of that State under the Convention, where substantial grounds have been shown for believing that the person in question would, if extradited, face a real risk of being subjected to treatment contrary to Article 3 in the receiving country. … Nonetheless, there is no question of adjudicating on or establishing the responsibility of the receiving country, whether under general international law, under the Convention or otherwise. *In so far as any liability under the Convention is or may be incurred, it is liability incurred by the extraditing Contracting State by reason of its having taken action which has as a direct consequence the exposure of an individual to proscribed ill-treatment.*[140]

The same logic applies here. It is immaterial that the eventual harm would be produced by the actions of another party to the conflict which might attack the directly participating civilians. What matters for the purposes of establishing the international responsibility of the acting State is that its actions have as a direct consequence the exposure of an individual to a real risk of proscribed effects.

What might such proscribed effects be in our present context? The right to life, as explained by the UN Human Rights Committee, "concerns the entitlement of individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death".[141] It is generally accepted that the relevant protections continue to apply during armed conflict, including in the conduct of hostilities.[142] In this regard, it is crucial that the encouragement of

139 See the above section on "Loss of Protection from Attack and the Related Safeguards".

140 ECtHR, *Mamatkulov and Askarov v. Turkey*, Appl. Nos 46827/99, 46951/99, Judgment (Merits and Just Satisfaction) (Grand Chamber), 4 February 2005, para. 67 (emphasis added).

141 General Comment 36, above note 138, para. 3.

142 *Ibid.*, para. 64. See also ICRC Interpretive Guidance, above note 15, p. 11, noting that the Guidance deals with direct participation in hostilities under an IHL lens only, without prejudice to other bodies of law – such as IHRL – that may concurrently be applicable in a given situation.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

civilians to directly participate in hostilities has been shown to be potentially inconsistent with several obligations under IHL.[143] As explained by the Committee, "practices inconsistent with international humanitarian law, entailing a risk to the lives of civilians and other persons protected by international humanitarian law, … would also violate article 6 of the [International Covenant on Civil and Political Rights]".[144]

It is useful at this point to distinguish the involvement of civilians in hostilities from the conscription of civilians into the armed forces of States. The latter is an inherent right of States, including where they do so on a compulsory (forced) basis.[145] The legal status under IHL of individuals who are recruited into armed forces changes from "civilian" to "combatant".[146] This transformation thus brings about key entitlements that are associated with combatant status, including immunity from prosecution for participating in hostilities and entitlement to prisoner-of-war status if captured. Therefore, even though recruitment into armed forces also entails a risk to the lives of the concerned individuals, these no longer qualify as civilians and the acceptance of such risk is an established feature of IHL.[147]

And yet, it would be overbroad to suggest that all forms of encouragement of civilians to engage in cyber activities that constitute direct participation in hostilities amount to a violation of the concerned individuals' right to life. In the IHRL jurisprudence, relevant criteria include whether the activity at issue is dangerous by its very nature and puts the life of the people concerned at real and imminent risk.[148] While this may be the case with some activities discussed in this article – such as using one's phone to transmit tactical intelligence directly from the front line (scenario 2) – others may be inherently less dangerous.

In general terms, whenever a State undertakes or organizes dangerous activities, or authorizes them, it must ensure that the risk is reduced to a reasonable minimum.[149] Applied to the present context, this means that States should prioritize those forms of civilian involvement in the war effort that do not place these individuals in harm's way. This would include cyber activities, which merely build up or maintain the military capacity of a party to the conflict, given that – as noted earlier – these types of conduct do not qualify as direct participation in hostilities.[150]

143 See the above section on "Legal Implications for States: International Humanitarian Law".
144 General Comment 36, above note 138, para. 64.
145 Diakonia, *Forcible Recruitment of Adults by Non-State Armed Groups in Non-International Armed Conflict*, Legal Brief, May 2019, p. 3.
146 Y. Dinstein, above note 92, pp. 199–200.
147 See e.g. M. Sassòli, above note 108, p. 2; Y. Dinstein, above note 92, pp. 199–200.
148 ECtHR, *Nicolae Virgiliu Tănase v. Romania*, Appl. No. 41720/13, Judgment (Grand Chamber), 25 June 2019, para. 140.
149 ECtHR, *Mučibabić v. Serbia*, Appl. No. 34661/07, Judgment (Third Section), 12 July 2016, para. 126 (concerning the death of eleven individuals in the context of covert production of rocket fuel under the auspices of a government intelligence service).
150 See text at above note 34.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

In addition, the protection of individuals' lives under the IHRL framework must strike a balance with the protection of personal autonomy, which is an inherent part of the right to respect for private life.[151] In order for individuals to exercise this autonomy, States should take adequate measures to provide them with information enabling them to assess the relevant risks to their physical integrity.[152] If the acting State furnishes the concerned individuals with full information about the risks entailed in engaging in a cyber or digital activity that may amount to direct participation in hostilities and they nonetheless decide to do so, it would be more difficult to argue that the State has exposed them to unacceptable risk from the perspective of their right to life.

In the final analysis, it is impossible to draw general conclusions as to the compatibility of the practices considered here with IHRL. The most extreme forms – such as requesting civilians to act in ways that would expose them to the real and imminent danger of being directly attacked, and without informing them of this risk – would most likely violate the concerned individuals' right to life. For instance, asking unwitting civilians who find themselves in the theatre of hostilities to use their phones to supply tactical intelligence needed for immediate attacks would be highly problematic.

However, lesser forms of involvement may more helpfully be analogized to activities such as State-encouraged voluntary participation in dangerous activities like environmental or industrial disaster response. Provided that, for example, volunteer firefighters are given accurate information about the risks they might be facing in helping to extinguish a massive fire, and provided that the State takes reasonable risk mitigation measures, it would be a stretch to argue (on IHRL grounds) that the State was precluded from requesting their assistance, particularly if there was a lack of professional personnel available.

It is submitted that the same approach should apply to the encouragement of civilians to engage in cyber activities that may constitute direct participation in hostilities during armed conflicts. One would be hard-pressed to identify a blanket prohibition of such practices in IHRL, but at least some of them are problematic from the perspective of that body of law, and, generally speaking, if States have other ways of achieving their goals, they should prioritize those in order to avoid potential liability for human rights violations.

151 ECtHR, *Lambert and Others v. France*, Appl. No. 46043/14, Judgment (Grand Chamber), 5 June 2015, para. 142.

152 See e.g. ECtHR, *Öneryıldız v. Turkey*, Appl. No. 48939/99, Judgment (Grand Chamber), 30 November 2004, para. 108 (substantiating a finding of a violation of the right to life – in the context of dangerous industrial activities – in part on the fact that the State had "not shown that any measures were taken in the instant case to provide the [applicants] with information enabling them to assess the risks they might run as a result of the choices they had made"); ECtHR, *L.C.B. v. United Kingdom*, Appl. No. 14/1997/798/1001, Judgment, 9 June 1998, para. 38 (considering that a State may violate its obligation to safeguard the right to life if it does not inform individuals under its jurisdiction about a real risk to their health that is known to that State). See also ECtHR, *Vilnes and Others v. Norway*, Appl. Nos 52806/09, 22703/10, Judgment (First Section), 5 December 2013, paras 233–245 (holding that the State violated the applicants' right to respect for their private life by failing to ensure that they received essential information enabling them to assess the risks to their health and safety entailed in a dangerous activity authorized by the State).

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press

Conclusion

The ongoing process of digitalization of societies is transforming the way in which wars are fought. States have added cyber capabilities to their military arsenals and continue to search for the most effective ways of projecting their cyber power, including during armed conflicts. One of the concerning trends in this regard relates to the growing involvement of civilians in activities on the digital battlefield.

This article has demonstrated that – even though the circumstances when this occurs are quite narrow – some forms of such involvement may qualify as direct participation in hostilities under IHL. While individuals who engage in these activities do not automatically violate international law, they must be aware that doing so temporarily removes their protection from direct attack. States that decide to encourage such engagement should therefore at the very least be open and transparent about what it means in practical and legal terms.

Moreover, certain acts that put civilians in harm's way by making them directly participate in hostilities may constitute standalone violations of IHL and IHRL obligations by the acting States. From the IHL perspective, the relevant rules include the obligations of constant care and passive precautions, and certain obligations relating to the protection of children. From the perspective of IHRL, some extreme forms of civilian involvement may implicate those individuals' right to life. States must not engage in such conduct in order to comply with their duties under international law.

Beyond these specific prescriptions, the encouragement of civilian involvement in the conduct of hostilities contributes to the erosion of the principle of distinction, an edifice on which the rest of the law applicable in armed conflicts is built. Accordingly, it is strongly recommended for States to reverse the trend of civilianization of the digital battlefield and to refrain as much as possible from involving civilians in the conduct of cyber hostilities. After all, it is a basic truth that "[t]hings fall apart [when] the centre cannot hold".[153]

153 W. B. Yeats, "The Second Coming", 1919.

https://doi.org/10.1017/S1816383123000152 Published online by Cambridge University Press