



# **INTERNATIONAL HUMANITARIAN LAW AND THE GROWING INVOLVEMENT OF CIVILIANS IN CYBER OPERATIONS AND OTHER DIGITAL ACTIVITIES DURING ARMED CONFLICT**

**REPORT OF A RESEARCH AND EXPERT CONSULTATION PROJECT OF  
THE JOINT INITIATIVE ON THE DIGITALIZATION OF ARMED CONFLICT**

Report drafted by Anna Greipl, Research Assistant, Geneva Academy of International Humanitarian Law and Human Rights; Samit D'Cunha and Tilman Rodenhäuser, Legal Advisers, International Committee of the Red Cross (ICRC); Laurent Gisel, Head of Arms and Conduct of Hostilities Unit, ICRC; Marco Roscini, Swiss Chair of International Humanitarian Law, Geneva Academy of International Humanitarian Law and Human Rights (2022–2024) and Professor of International Law, University of Westminster.

*Citation:* International Committee of the Red Cross and Geneva Academy of International Humanitarian Law and Human Rights, *International Humanitarian Law and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities During Armed Conflict*, Geneva, ICRC, November 2025.

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>EXECUTIVE SUMMARY.....</b>   | <b>2</b>  |
| <b>INTRODUCTION .....</b>   | <b>5</b>  |
| <b>1. CIVILIAN INVOLVEMENT IN CYBER OPERATIONS AND OTHER DIGITAL ACTIVITIES<br/>DURING ARMED CONFLICT.....</b>                  | <b>6</b>  |
| Growing civilian involvement: A shift in the digital space? .....   | 6         |
| Forms of civilian involvement .....   | 8         |
| <b>2. IHL AND INDIVIDUAL CIVILIANS INVOLVED IN CYBER OPERATIONS<br/>AND OTHER DIGITAL ACTIVITIES DURING ARMED CONFLICT.....</b> | <b>9</b>  |
| The regulation under IHL of civilian cyber operations<br>and other digital activities in the context of an armed conflict ..... | 9         |
| The responsibility of states to ensure respect for IHL .....  | 10        |
| The legality under IHL of parties to an armed conflict<br>encouraging civilians to participate in hostilities .....             | 10        |
| Digital activities by civilians and the notion<br>of ‘direct participation in hostilities’ .....                                | 12        |
| <b>3. IHL AND HACKER GROUPS IN CONTEMPORARY ARMED CONFLICT .....</b>  | <b>15</b> |
| The legal status of hacker groups and their members in international armed conflict .....                                       | 15        |
| The legal status of hacker groups in non-international armed conflict.....  | 16        |
| The risk for civilian hackers of losing protection against attack .....   | 17        |
| Ensuring respect for IHL when hacker groups conduct cyber operations<br>in the context of an armed conflict .....               | 18        |
| <b>4. IHL AND PRIVATE TECHNOLOGY COMPANIES’ SERVICES<br/>AND OPERATIONS IN ARMED CONFLICT.....</b>                              | <b>19</b> |
| IHL protection for the personnel and property of private technology companies .....   | 19        |
| Ensuring that private technology companies’ operations respect IHL.....   | 21        |
| <b>THE NEED FOR FURTHER STUDY AND DIALOGUE .....</b>  | <b>22</b> |
| <b>EXPERTS WHO PARTICIPATED IN THE EXPERTS’ MEETING RELATED TO THIS REPORT .....</b>  | <b>23</b> |

# EXECUTIVE SUMMARY

For centuries, civilians have been involved – to a greater or lesser degree – in activities closely linked to hostilities during armed conflict. Because of the strategies of ‘total defence’ and ‘comprehensive defence’ – which entail mobilizing the ‘whole of society’ in the defence of a nation – civilian involvement in armed conflict might become more extensive. With the rapid digitalization of our world and the way in which wars are fought, the involvement of civilians in armed conflicts can take new forms, become easier for civilians, and the related risks reach a new scale. Indeed, in some recent armed conflicts civilians have been encouraged to collect militarily relevant information at scale through government-provided apps; unprecedented numbers of civilian hacker groups (often referred to as ‘hacktivists’) have conducted cyber operations against whoever they consider the enemy; and technology companies have provided services and infrastructure to belligerents, at times unaware of the risks to company assets, staff, and customers. This trend has serious implications for the safety of civilians during armed conflict.

As part of a joint initiative, entitled “Digitalization of Conflict: Humanitarian Impact and Legal Protection”, by the International Committee of the Red Cross (ICRC) and the Swiss Chair of International Humanitarian Law (IHL) at the Geneva Academy of International Humanitarian Law and Human Rights, we conducted in-depth research and consulted experts, including in an experts’ meeting hosted in Geneva, in an effort to explore and clarify how IHL addresses the involvement of civilians in cyber and other digital activities during armed conflicts, with a view to limiting the human cost of this worrying trend.

This report concludes that conducting cyber and other digital activities in the context of armed conflicts exposes civilians to a significant risk of harm. It discusses specific legal questions that arise as a result of such activities and presents how respect for IHL can play an important role in avoiding or minimizing those risks. Finally, the report focuses on the activities of individuals, hacker groups, and private technology companies.

This report aims to contribute to a shared understanding of the application of IHL in the information and communication technology (ICT) environment. It strives to increase legal clarity, highlight issues that demand further attention, and ultimately prevent harm that may result from cyber operations and other digital activities during armed conflicts. The findings presented in the report show, among other things, (1) the need for states to further address the growing civilian involvement in cyber operations and other digital activities in armed conflicts, including by taking measures to ensure IHL is respected; (2) for individuals, hacker groups, and technology companies to be aware of relevant risks and obligations; and (3) for legal and other experts to continue analysing this development.

Some of the issues discussed in this report were addressed, in 2024, by states and members of the International Red Cross and Red Crescent Movement in Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, titled “Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict”. The report presents a detailed explanation of these topics from a legal perspective. Discussion of some of these issues has also begun to take place (and will continue into 2026) in the ICT Workstream of the Global Initiative to Galvanize Political Commitment to International Humanitarian Law. It is hoped that the report will help inform and enrich those deliberations.

## KEY RISK FOR CIVILIANS, AND OBLIGATIONS FOR CIVILIANS AND STATES

- 1. The digitalization of our societies has contributed to a growing involvement of civilians in cyber operations and other digital activities during armed conflicts.** This trend has serious implications because it makes it factually more difficult to distinguish between combatants and military objectives on the one hand, and civilians and civilian objects on the other, and puts the latter at risk of being misidentified as lawful targets or incidentally harmed. To avoid such risks:

  - States should – to the extent feasible – avoid involving civilians in activities that bring them close to hostilities, and if they decide to involve them, give due consideration to the risks this would expose civilians to.
  - If states intend to use civilians in activities that bring them close to hostilities, they should integrate such civilians into their armed forces, or at least inform them of the relevant risks and their obligations.
- 2. Civilian hackers must respect IHL when they operate in the context of armed conflicts.** IHL applies to the acts of individuals when those acts take place in the context of, and are associated with, an armed conflict. This is regardless of whether those activities are conducted by individual civilian hackers, civilians acting as part of a hacker group, employees of technology companies, or any civilian acting on behalf of a party to the conflict.

  - If civilians conduct cyber operations in the context of armed conflicts, they must seek information about the limits that IHL imposes on such operations, develop a sufficient understanding of these limits, and respect them.
  - In particular, they must respect the principles of distinction, proportionality and precaution, and the specific protection afforded to certain categories of persons and objects.
- 3. Parties to armed conflict, whether state or non-state armed groups, must respect IHL and ensure respect for it by any person or group that forms part of their armed forces or by other persons or groups acting on their instructions or under their direction or control; furthermore, states have a due diligence obligation to prevent IHL violations by all civilians within their jurisdiction, including civilian hackers, hacker groups and technology companies.** This long-standing obligation is particularly relevant with regard to the involvement of civilians in armed conflicts.

  - Parties to armed conflict – state or non-state – must ensure respect for IHL by all of their agents and actors whose conduct is attributable to them, and must not encourage civilians to violate IHL or aid or assist such violations.
  - States should make IHL known, as necessary and feasible, to civilian hackers, hacker groups, and employees of private technology companies, demand that they respect IHL, and take the measures necessary to suppress IHL violations and prosecute those who commit war crimes.
- 4. Private technology companies must be aware that operating in situations of armed conflict, and providing services or infrastructure to the parties to the armed conflict, has legal and practical implications.** Notably, certain activities, such as defending military networks against cyber operations, could amount to direct participation in hostilities by their employees, and in certain cases their assets may become military objectives and liable to attack.

  - Private technology companies that operate in an armed conflict, and provide digital services related to it, should familiarize themselves with IHL, understand how their services and activities may expose their staff, assets, and customers to harm, and take effective measures to minimize those risks.
  - To prevent or minimize incidental damage to civilian objects and customers resulting from an attack on a military objective, private technology companies should, to the extent feasible, segregate the parts of their assets that are used by militaries from those used by civilian customers.



- 5. Civilians must be aware of the risk that conducting cyber operations and other digital activities during armed conflicts may expose them to harm. Under IHL, civilians lose protection against attack only if they directly participate in hostilities: parties to armed conflict must carefully assess when this might be the case and must act on the presumption that it is not.** Under IHL, a civilian hacker conducting cyber operations to disrupt a party to the conflict's military operations will likely directly participate in hostilities and lose protection against attack, but only for the duration of the operation. In contrast, although the widespread use of smartphones has enabled civilians to gather and share militarily relevant information with armed forces, the mere fact of a civilian using a smartphone near a site of hostilities does not amount to 'direct participation in hostilities'.
- Civilians must be aware – and states should make them aware – that hacking in support of a party to an armed conflict and to the detriment of an adversary, or collecting militarily relevant information for a belligerent, might put them at risk of real harm.
  - In case of doubt, belligerents must presume that civilians are protected against attack. For instance, in practice it will be difficult for an attacker to know for what purpose individuals are using their phones in places where hostilities are taking place.

# INTRODUCTION

This report is part of a joint initiative, entitled “Digitalization of Conflict: Humanitarian Impact and Legal Protection”, by the ICRC and the Swiss Chair of International Humanitarian Law at the Geneva Academy of International Humanitarian Law and Human Rights. As part of this initiative, we conducted in-depth research and consulted experts, including during an experts’ meeting hosted in Geneva, to explore and clarify how IHL addresses the involvement of civilians in cyber and other digital activities during armed conflicts. Experts from different parts of the world, with relevant professional backgrounds in different fields, participated in this work, alongside representatives from the ICRC and the Geneva Academy.<sup>1</sup>

The Geneva Academy and the ICRC are the sole authors of the report. Its findings do not necessarily represent the consensus, or individual views, of the experts consulted. Addressed primarily to legal advisers, political decision makers, academics, researchers, and civilians who may get involved in digitalizing armed conflicts, the report aims to provide a preliminary understanding of the legal challenges and risks related to civilian involvement in cyber operations and other digital activities during armed conflicts.

---

<sup>1</sup> A list of experts who took part in this work is included at the end of this report.

## CHAPTER 1

# CIVILIAN INVOLVEMENT IN CYBER OPERATIONS AND OTHER DIGITAL ACTIVITIES DURING ARMED CONFLICT

Albeit at different rates, societies throughout the world are digitalizing. In armed conflicts, connectivity and the availability of ICTs has significant and at times life-saving value for civilian populations. At the same time, during armed conflicts ICTs are used as a means and method of warfare, and have become a means for growing civilian involvement in cyber operations and other digital activities in armed conflicts (hereafter “civilian involvement”).<sup>2</sup> This trend has serious implications for civilians and civilian objects, as it may expose them to significant harm. On the one hand, civilians involved in armed conflicts risk losing protection against attack – or of being misperceived to be losing protection – and of being injured or killed as a result. Such attacks may also put other civilians at risk of being incidentally harmed. On the other hand, too often civilians who conduct cyber operations target civilian objects and disrupt civilian life in societies, unaware of their legal obligations.

To avoid giving rise to these risks, or to mitigate them, a clear understanding of key IHL questions is needed. To uphold the protection of civilians and civilian objects, we must further clarify the limited circumstances in which civilians undertaking activities in the ICT environment may be considered to be ‘directly participating in hostilities’, and the circumstances in which an object, such as a civilian network or data centre that is used during an armed conflict, becomes a ‘military objective’ under IHL. Regarding the need to ensure that civilians respect IHL, the obligations of states when civilians become involved in cyber operations and other digital activities are particularly important.

### GROWING CIVILIAN INVOLVEMENT: A SHIFT IN THE DIGITAL SPACE?

For centuries, civilians have been involved – to a greater or lesser degree – in activities closely linked to hostilities during armed conflict. This is the result of a confluence of factors, such as the changing nature of armed conflicts and, more recently, the digitalization of societies. For example, parties rely on or make use of civilian ICT infrastructure for their military operations, or outsource traditional military functions to private contractors and other civilians.<sup>3</sup>

The digitalization of societies – including those affected by armed conflict – has accelerated civilian involvement, and related risks, in at least two ways.

<sup>2</sup> See ICRC, Statement delivered at the 77th session of the United Nations General Assembly, First Committee General Debate on all disarmament and international security agenda items (12 October 2022), which notes that “the growing involvement of civilians and civilian companies in military cyber operations and other digital activities during armed conflict exposes them to harm and risks undermining the principle of distinction”; see also Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, “Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict” (31 October 2024, adopted by consensus): [https://rcrcconference.org/app/uploads/2024/10/34IC\\_R2-ICT-EN.pdf](https://rcrcconference.org/app/uploads/2024/10/34IC_R2-ICT-EN.pdf), preambular paras 7–14.

<sup>3</sup> For an in-depth discussion of the IHL obligations of private military and security companies, see Emanuela-Chiara Gillard, “Business goes to war: Private military/security companies and international humanitarian law”, *International Review of the Red Cross* (IRRC), Vol. 88, No. 863, September 2006, p. 525.



First, the digitalization of societies has generated new vulnerabilities in armed conflict. The ‘attack surface’ in the ICT infrastructure of societies has vastly increased – digital devices, mobile-phone applications, and networks are almost everywhere nowadays – and a growing number of essential civilian services rely on ICTs. Civilians and militaries often use the same digital infrastructure. As a result, ICTs and the civilian infrastructure and services they support face a growing risk of harm through cyber operations.

Second, the wide availability of connectivity and digital tools and services has lowered the barriers for civilians to engage in activities related to armed conflicts.<sup>4</sup> It has reshaped the concept of distance: individuals can operate far from where hostilities take place and also have a direct impact on parties to the conflict and on civilian populations affected by armed conflict. The nature of the internet has also simplified scaling up civilian involvement, as hacker groups can be assembled, and coordinated, online very quickly now.

Civilian involvement in armed conflict can have serious implications for civilian populations. It risks generating confusion about who or what is ‘civilian’ and must not be attacked, and who or what is a ‘military objective’. As a result, it increases the risk of erroneous or unlawful attacks. Even attacks against military objects will likely harm civilians and civilian objects, either those in close physical proximity to the digital infrastructure attacked, or those digitally connected to the attacked objects. Such attacks also risk disrupting the provision of essential services that rely on the targeted ICT infrastructure, with immediate consequences for civilian populations. These risks underscore the need to identify the protection afforded by IHL to civilians and civilian ICT infrastructure. In addition, further clarity is needed on the legal obligations of civilians and parties to conflict when civilians conduct such cyber operations; clarity is also needed on the different forms of civilian involvement during armed conflict that may put civilians and civilian objects at risk of losing their protection against attack.

The analysis in this report focuses on IHL questions raised by the growing involvement of civilians in cyber operations and other digital activities during international and non-international armed conflicts. States also have legal obligations under other fields of international law which are relevant to civilian involvement in armed conflict, most notably under the law on the use of force, the law of neutrality, international human rights law, international criminal law, and international law on state responsibility. For example, even if the view is taken that certain forms of civilian involvement through cyber and other digital activities may make a person or object in a state that is not party to an armed conflict lose the protection they would be afforded by IHL, any attack on such a person must comply with all applicable rules of international law, in particular the strict limits imposed by the Charter of the United Nations. Those questions will, however, not be addressed in this report unless they are of relevance in discussing specific IHL issues.

---

<sup>4</sup> See, e.g., Kubo Mačák, “Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield”, *IRRC*, Vol. 105, No. 923, August 2023, p. 968; Jonathan Horowitz, “One click from conflict: Some legal considerations related to technology companies providing digital services in situations of armed conflict”, *Chicago Journal of International Law*, Vol. 24, No. 2, 2024; and Tilman Rodenhäuser, “Civilian hackers in war: The limits that international humanitarian law imposes on ‘volunteer IT armies’, ‘hacktivists’, and other civilian hackers”, *IRRC* (forthcoming).

## FORMS OF CIVILIAN INVOLVEMENT

Civilian involvement takes many forms. Civilians may become involved as individuals by conducting a cyber operation against a certain target. For instance, civilians have engaged in offensive cyber operations such as “distributed denial-of-service” (DDoS)<sup>5</sup> or cyber operations that aim at disrupting services or infrastructure associated with an adversary or its civilian population. Civilians have also engaged in defensive digital activities or have been involved in the gathering and sharing of information of military value.

Civilians can also be involved in cyber and other digital activities in the context of an armed conflict as part of a group. Some hacker groups are professionally organized or even state-sponsored; others operate independently and have varying degrees of internal organization; while others are loosely organized collectives.<sup>6</sup> In exceptional cases, such groups may become parties to armed conflict. While many of them conduct cyber operations in the context of armed conflicts, their understanding of and respect for the applicable rules of IHL is often limited or non-existent.

Civilians are also increasingly drawn into armed conflicts as employees of private technology companies, or affected as customers if the products or services of such companies become unavailable. In parallel, parties to armed conflicts employ or otherwise rely on private technology companies for some of their military activities, including cybersecurity, data management, communication and logistics.<sup>7</sup> Worryingly, in some instances, the same infrastructure and services – provided by private technology companies – that civilians rely on to access essential services is used, or relied upon, by parties to armed conflict to conduct military operations.

In this report, the different forms of civilian involvement described above are analysed in terms of the actors involved: individuals (Chapter 2), groups (Chapter 3), and private technology companies (Chapter 4). The legal issues overlap in some cases, but the report was structured like this to facilitate analysis and identify legal and policy measures in connection with each actor, with a view to preventing or mitigating the risks to them that might arise.

<sup>5</sup> “DDoS attacks” (this nomenclature does not suggest that such activities are necessarily attacks under IHL) aim to make a machine or network resource unavailable by flooding it with requests from compromised systems. See Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 210–211.

<sup>6</sup> Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law*, Oxford University Press, Oxford, 2018, pp. 104–108; Stefan Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, Center for Security Studies (CSS) ETH Zurich, Zurich, 2022, p. 1.

<sup>7</sup> Horowitz, “One click from conflict” (cited in footnote 4 above).

**CHAPTER 2**

# IHL AND INDIVIDUAL CIVILIANS INVOLVED IN CYBER OPERATIONS AND OTHER DIGITAL ACTIVITIES DURING ARMED CONFLICT

When civilians take part in cyber operations or other digital activities during armed conflict, three overarching questions arise. First, what rules are these individuals bound by and who is responsible for ensuring compliance? Second, does IHL permit involving civilians in cyber and other digital activities in the context of an armed conflict? And third, in what circumstances does such involvement put them in danger of being harmed?

## THE REGULATION UNDER IHL OF CIVILIAN CYBER OPERATIONS AND OTHER DIGITAL ACTIVITIES IN THE CONTEXT OF AN ARMED CONFLICT

Civilians conducting cyber operations in the context of an armed conflict must comply with IHL. Any cyber operation qualifying as an attack under IHL, and conducted in the context of an armed conflict, is subject to the IHL principles and rules of distinction, proportionality, and precautions. As there is currently no consensus among states and legal experts on the kinds of cyber operations that qualify as attacks under IHL,<sup>8</sup> it is important to emphasize that IHL also imposes limits on cyber operations that do not amount to an ‘attack’, such as the prohibition under IHL on directing cyber operations against civilian objects and the obligation to take constant care to spare the civilian population, civilians and civilian objects.<sup>9</sup> In addition, certain entities are afforded specific protection under IHL, such as medical services, humanitarian operations, and objects indispensable to the survival of the civilian population. In other words, these civilian entities enjoy protections against a range of harmful operations that do not qualify as attacks under IHL or may not otherwise be prohibited if conducted against civilians.

---

8 For an explanation of the legal debate on the notion of ‘attack’ under IHL in relation to cyber operations, and an overview of state positions on the subject, see Cyber Law Toolkit, “Attack (International Humanitarian law)”: [https://cyberlaw.ccdcoe.org/wiki/Attack\\_\(international\\_humanitarian\\_law\)](https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law)).

9 Arts 48 and 57, Protocol II additional to the Geneva Conventions (Additional Protocol II); Rule 15, ICRC Customary IHL Study <https://ihl-databases.icrc.org/en/customary-ihl/v1>. See also Rodenhäuser, *Organizing Rebellion* (cited in footnote 4 above); and Roy Schöndorf, “Israel’s perspective on key legal and practical issues concerning the application of international law to cyber operations”, *International Law Studies*, Vol. 97, No. 1, 2021, p. 401, which states that parties to armed conflict “cannot blatantly disregard such harmful effects [i.e. danger] to the civilian population in their military operations”.

## THE RESPONSIBILITY OF STATES TO ENSURE RESPECT FOR IHL

Under IHL, states have a due diligence obligation to prevent IHL violations by civilians over whom they exercise authority.<sup>10</sup> This is an obligation of conduct, not of result: while a state cannot prevent all IHL violations, it must take all feasible measures to do so.

This obligation should be further clarified through a set of good practices that states could adopt. While states should – to the extent feasible – be careful not to encourage civilians to take part in armed conflict, they could also develop educational and other measures for disseminating knowledge of IHL rules applicable to cyber operations and other digital activities conducted by civilians, and for raising awareness of relevant risks. These could take various forms, such as sharing of information about IHL rules via social media, dedicated apps, radio or other means of mass communication; or development of IHL-compliant model codes of conduct that cyber groups should be asked to comply with. The objective would be to reach civilians who are engaged in relevant activities.<sup>11</sup> Such measures would be a way of contributing to the implementation of states' legal obligation to disseminate knowledge of IHL – including the rules applicable to cyber operations – as widely as possible.<sup>12</sup>

When violations of IHL occur, states are under an obligation to suppress them and prosecute alleged offenders if required.<sup>13</sup> Domestic courts therefore play an important role in enforcing IHL and preventing impunity. With respect to cyber operations, the adoption of domestic laws or regulations criminalizing cyber operations in violation of IHL is required. These must be enforced and, where relevant, allegations of violations must be investigated and perpetrators prosecuted, particularly with regard to war crimes carried out by cyber means.<sup>14</sup> States should inform civilian hackers on their territory, or within their jurisdiction, of legal measures they may face – just as some states inform their citizens of the risks and legal consequences of physically participating in armed conflicts in other countries.

## THE LEGALITY UNDER IHL OF PARTIES TO AN ARMED CONFLICT ENCOURAGING CIVILIANS TO PARTICIPATE IN HOSTILITIES

While it has, at times, been argued that there is an “obligation on the part of civilians not to take a direct part in hostilities”<sup>15</sup> and that, if civilians do so, “they violate the law of war”,<sup>16</sup> it is largely accepted that – except for children (see below) – “IHL neither prohibits nor privileges civilian direct participation in hostilities”.<sup>17</sup> Civilians “were never meant to directly participate in hostilities on behalf of a party to the conflict”,<sup>18</sup> however, there is no express prohibition under IHL against their doing so.<sup>19</sup>

<sup>10</sup> See ICRC, *Commentary on the Third Geneva Convention*, 2020, para. 183 on Art. 1 <https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-1/commentary/2020?activeTab=1949GCs-APs-and-commentaries>.

<sup>11</sup> An example of such a selection of IHL rules that are particularly relevant to civilian hackers are the eight rules for hackers during war published by the ICRC. See ICRC, “Eight rules for ‘civilian hackers’ during war, and four obligations for states to restrain them”: <https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them>.

<sup>12</sup> Rules 142 and 143, ICRC Customary IHL Study.

<sup>13</sup> Arts 49, 50, 129 and 146, First, Second, Third and Fourth Geneva Conventions; Art. 85, Protocol I additional to the Geneva Conventions (Additional Protocol I).

<sup>14</sup> For more on this, see the discussion in this chapter. See also, in particular, Permanent Mission of Lichtenstein to the United Nations, *The Council of Advisers’ Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*, 2021.

<sup>15</sup> United States, *International Law – The Conduct of Armed Conflict and Air Operations: Air Force Pamphlet 110–31*, Judge Advocate General, Department of the Air Force, November 1976, pp. 5–8.

<sup>16</sup> 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, England, 2007, p. 122.

<sup>17</sup> ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, p. 44. There is an exception to this for civilians who are children: IHL requires that children must not be allowed to take part in hostilities (Rule 137 of the ICRC Customary IHL Study).

<sup>18</sup> ICRC *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, ICRC, Geneva, 2009, pp. 38–39.

<sup>19</sup> This view is shared by the *Tallinn Manual 2.0* group of experts, who have noted that IHL “does not bar any category of person from participating in cyber operations”. Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, England, 2017, Rule 86.

Some parties to armed conflict encourage civilians to involve themselves in military activities. This puts such civilians at risk of harm and raises legal questions. For example, parties must, “to the maximum extent feasible”, take the precautions necessary “to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations”.<sup>20</sup> The development and promotion, by parties to the conflict, of digital means that enable scaling up civilians’ participation in cyber and other digital activities – with a sizeable part of the population potentially losing their protection against attack under IHL because of (mis)perceptions that they had lost such protection, or being put at risk of incidental harm – requires careful consideration under this rule.<sup>21</sup> In addition, encouraging civilians to conduct cyber operations that violate IHL is unlawful: for example, IHL prohibits encouraging civilians to conduct cyber attacks against other civilians or civilian objects.<sup>22</sup>

The obligation that a party takes constant care to spare the civilian population, civilians, and civilian objects in the conduct of military operations further suggests an obligation to at least inform and warn civilians about the harmful consequences of the activities they are prompted, encouraged, or incentivized to conduct. Additionally, concrete recommendations for measures civilians can take, to protect themselves against the harmful consequences of their participation in hostilities, should be provided. In practice, this could include ensuring that smartphone applications that enable civilians to provide militarily relevant information specify (during the download, installation process, and use) the risks and legal consequences that the use of the applications can have, and concrete measures to avoid or at least mitigate such risks.

While IHL does not prohibit direct participation in hostilities by adult civilians, it does, together with applicable human rights law, prohibit the direct, and sometimes the indirect, participation of child civilians in hostilities.<sup>23</sup> As a result, measures specifically addressing the protection of children are necessary where participation in armed conflicts is made possible through widely accessible digital means, be it hacking tools or online communication tools and platforms. The obligation to take such measures arise from a warring party’s duty to take all feasible measures to prevent children from participating in hostilities,<sup>24</sup> and could consist of parties implementing additional constraints on children’s access to certain digital tools that can be used to participate in hostilities.<sup>25</sup> Not doing so may result in a violation of the relevant IHL rules on the protection of children.

<sup>20</sup> Art. 58, Additional Protocol I.

<sup>21</sup> A similar logic may be supported by the right to life under international human rights law, which, according to the United Nations Human Rights Committee, entitles “individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death”. See UN Human Rights Committee, “General Comment No. 36 on Article 6: Right to Life”, UN Doc. CCPR/C/GC/36 (3 September 2019), para. 3.

<sup>22</sup> Art. 1 common to the Geneva Conventions. See Chapter 3 below. See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, p. 76: <https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-recommitting-to-protection-in-armed-conflict-on-the-70th-anniversary-of-the-geneva-conventions-pdf-en>; see also Tilman Rodenhäuser, “The legal boundaries of (digital) information or psychological operations under international humanitarian law”, *International Law Studies*, Vol. 100, No. 541, 2023, pp. 552–556.

<sup>23</sup> Art. 77(2), Additional Protocol I; Art. 4(3)(c), Additional Protocol II; Art. 4(1), Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict; Art. 22(2), African Charter on the Rights and Welfare of the Child; Rule 137 of the ICRC Customary IHL Study.

<sup>24</sup> Art. 77(2), Additional Protocol I; Art. 4(3)(c), Additional Protocol II; Art. 4(1), Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict; Art. 22(2), African Charter on the Rights and Welfare of the Child, which refers to “all necessary measures”; Rule 136 of the ICRC Customary IHL Study.

<sup>25</sup> Mačák, “Will the centre hold?” (cited in footnote 4 above), pp. 986–987.

## DIGITAL ACTIVITIES BY CIVILIANS AND THE NOTION OF 'DIRECT PARTICIPATION IN HOSTILITIES'

Although the notion of 'direct participation in hostilities' is critical for legally assessing the risks faced by civilians, it is not defined in IHL.<sup>26</sup> Deciding whether a civilian is 'directly participating in hostilities' is relevant to determining whether they are protected from direct attack under IHL or whether they have lost this protection. After extensive research and consultations with experts, the ICRC has found that for an act to amount to 'direct participation in hostilities', three criteria must be met cumulatively: (1) threshold of harm, (2) direct causation and (3) belligerent nexus.<sup>27</sup>

- The threshold of harm is met when an act is 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.
- Direct causation requires a direct causal link between that act and the harm likely to result either from it or from a coordinated military operation of which that act constitutes an integral part.
- To meet the criterion of belligerent nexus, 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.<sup>28</sup>

The following paragraphs present key challenges related to the application of each criterion in the context of cyber and other digital activities. It is worth noting at the outset that loss of protection against direct attack within the meaning of IHL is not a punishment for possible criminal behaviour, but a legal consequence based on the principle of military necessity in the conduct of hostilities.

Regarding the threshold of harm, several issues arise.

One is the concern that the harm done by acts that "adversely affect the military operations or military capacity of a party to an armed conflict" might be understood as a very low threshold in the context of cyber operations. A wide variety of civilian cyber activities during armed conflicts could be thought to meet this criterion.<sup>29</sup> For example, in addition to the killing and wounding of military personnel and causing physical or functional damage to military objects, the military operations or military capacity of a party to the conflict can also be adversely affected by cyber activities restricting or disrupting deployments, logistics, and communications.<sup>30</sup> Because of the risks for the protection of civilians, experts questioned whether further clarification may be needed on the type and effect of the digital activities that could be considered as 'adversely affecting the military operations or military capacity of a party to the conflict' for the purpose of the analysis of whether a civilian might be losing their protection against attack.

In this regard, it may be questioned whether the kinds of operations conducted by civilian hackers – in particular DDoS operations against civilian infrastructure, administration or companies – cause a type or

26 In 2009, to clarify the parameters of this concept, the ICRC published its *Interpretive Guidance*. See also Tallinn Manual 2.0 (cited in footnote 19), Rule 97, para. 95 ("The International Group of Experts generally agreed with the three cumulative criteria for qualification of an act as direct participation that are set forth in the ICRC Interpretive Guidance.").

27 ICRC, *Interpretive Guidance*, p. 46. The guidance reflects the ICRC's view on the meaning and application of the concept in both international and non-international armed conflict. The ICRC's *Interpretive Guidance* has been cited by, and before, several international and domestic courts and tribunals; referred to in states' military manuals and legal positions; and relied upon by some UN bodies. For a detailed list of examples, see Crawford 2021, pp. 214–215. However, it is not universally accepted and states and experts continue to disagree about certain aspects. See also, Michael N. Schmitt, "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A critical analysis", *Harvard National Security Journal*, Vol. 1, May 2010, p. 5; and Nils Melzer, "Keeping the balance between military necessity and humanity: A response to four critiques of the ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities*", *Journal of International Law and Politics*, Vol. 42, No. 3, p. 831: <https://nyujilp.org/wp-content/uploads/2012/04/42.3-Melzer.pdf>.

28 ICRC, *Interpretive Guidance*, p. 46.

29 ICRC, *Interpretive Guidance*, p. 48.

30 In the ICRC's *Interpretive Guidance*, experts took the view that "electronic interference with military computer networks could also suffice [to meet the harm threshold], whether through computer network attacks (CNA) or computer network exploitation (CNE)". See ICRC, *Interpretive Guidance*, p. 48.



level of harm that meets the required threshold of harm to qualify as ‘direct participation in hostilities’. The ICRC’s *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* provides that acts directed against civilians or civilian objects must be reasonably expected to cause death, injury, or destruction to meet the threshold of harm,<sup>31</sup> and that attacking a civilian object would meet this threshold. However, experts involved in drafting the ICRC’s *Interpretive Guidance* also held at the time that “the manipulation of computer networks” or even “the interruption of electricity, water, or food supplies” cannot be equated with the use of means or methods of “warfare” or regarded as “injuring the enemy”.<sup>32</sup> Under that view, some of the activities of civilian hackers may not meet the harm threshold.

It must also be recalled that, when considering whether a person is using their phone to transmit militarily relevant information, the starting point must be that phones are used by civilians for many purposes, primarily civilian ones. Civilians may collect and share information about military activities for a variety of reasons, including to warn their families or other civilians of the dangers arising from military activities or to collect evidence of crimes. In those situations, there is no harm caused, and no ‘belligerent nexus’, and therefore no ‘direct participation in hostilities’. Thus, soldiers who see a civilian using their phone to take pictures or videos of armed forces must not simply assume that the civilian would share such information with their enemy and potentially cause the required threshold of harm in support of one party to the conflict and to the detriment of another.

The application of the criterion of direct causation similarly poses questions, primarily in the context of the collection and sharing of militarily relevant information through apps. There might be cases in which the sharing, by civilians, of such information with the military meets the criterion of direct causation. This may be the case, for instance, where the information is provided to execute a specific hostile act, such as “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 attack that target”,<sup>33</sup> or when the information provided by civilians is the primary target information on which an attack is based, and there is a clear link between the time at which the information is provided and the attack.<sup>34</sup> In practice, even in these exceptional cases, it will likely be difficult to ascertain whether specific information is needed or used for targeting purposes.

Several challenges also exist for the application of the criterion that an act must show a belligerent nexus, meaning that an act performed by civilians, including cyber activities by civilian hackers, 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, and must therefore be “closely related to the hostilities conducted between parties to an armed conflict”.<sup>35</sup> For instance, in times of armed conflict, mere cyber criminality, even if that was causing significant harm, would not show a nexus to the conflict and would therefore not amount to direct participation in hostilities. Therefore, such cybercrimes would have to be addressed exclusively through law enforcement measures.<sup>36</sup> Likewise, forms of ‘civil unrest’ brought about through cyber or other digital means, but not conducted in support of one party to the conflict and to the detriment of another, would not amount to direct participation in hostilities, even if they cause harm.<sup>37</sup> It may also be questioned whether cyber operations by civilian hackers that disrupt civilian government services far away from the actual fighting, and without being specifically related to military operations – but still clearly motivated by the conflict – show the required belligerent nexus. In any case, even if the view is

<sup>31</sup> ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, p. 49.

<sup>32</sup> ICRC, *Interpretive Guidance*, p. 50.

<sup>33</sup> Mačák, “Will the centre hold?” (cited in footnote 4 above), p. 974.

<sup>34</sup> See also Michael N. Schmitt and William Casey Biggerstaff, “Are civilians reporting with cell phones directly participating in hostilities?”: <https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/>.

<sup>35</sup> ICRC, *Interpretive Guidance*, p. 58.

<sup>36</sup> ICRC, *Interpretive Guidance*, p. 59. For further discussion of the nexus element, see Section II(i).

<sup>37</sup> ICRC, *Interpretive Guidance*, p. 63.

taken that such activities did not qualify as ‘direct participation in hostilities’, they would nonetheless be unlawful under IHL and must be suppressed or the perpetrators prosecuted (see above).

A challenge that arises with respect to all civilians involved in cyber or other digital activities in armed conflict, be they civilian hackers or employees of private technology companies (see below), is determining how the temporal element of ‘direct participation in hostilities’ would apply if a cyber operation against a belligerent is time-delayed. There is general agreement that the civilian may lose protection from attack when they initiate the operation; and many would agree that the temporal scope of the loss of protection in such a case would be limited to when the civilian has control over the deployment or effects of the operation.

In any circumstance where there is doubt about whether a person is a civilian or not, that person shall be considered to be a civilian.<sup>38</sup> Likewise, civilians must be presumed not to be directly participating in hostilities; they are therefore protected from attack.<sup>39</sup> Difficulties in operationalizing the legal presumption that civilians are not directly participating in hostilities<sup>40</sup> when using phones close to hostilities must not lead to a decision to attack such civilians. Likewise, the mere downloading or installing of a mobile phone application that can be used to report military activities, or that could support DDoS operations by a hacking group, is insufficient to be considered ‘direct participation in hostilities’, regardless of any subsequent background work the application undertakes. Rather, it is an individual’s specific use of the application that needs to be considered in any analysis of ‘direct participation in hostilities’. In this respect, parties to armed conflict should have clear rules of engagement that specify which operations are permissible in circumstances where such factual uncertainties exist, in order to ensure that the presumption of civilian status is respected.

---

<sup>38</sup> Art. 50, Additional Protocol I.

<sup>39</sup> See ICRC, *Interpretive Guidance*, pp. 75–76.

<sup>40</sup> This controversy is also reflected in *Tallinn Manual 2.0*, p. 432.

## CHAPTER 3

# IHL AND HACKER GROUPS IN CONTEMPORARY ARMED CONFLICT

The increasing involvement of hacker groups – including hacktivists – hackers-for-hire and cybercriminals – in armed conflicts necessitates a better understanding of the status and obligations under IHL of these groups and their members.

## THE LEGAL STATUS OF HACKER GROUPS AND THEIR MEMBERS IN INTERNATIONAL ARMED CONFLICT

In an international armed conflict (IAC), assessing whether an organized group or unit constitutes part of the armed forces of a belligerent state is important for at least three reasons. First, members of the armed forces (except for medical and religious personnel) are combatants. Attacks may be directed against them. Second, combatants, including members of the armed forces of a party to a conflict and members of certain groups who belong to a party to an armed conflict, become prisoners of war (POWs) as soon as they fall into the hands of the enemy and until their final release and repatriation. They benefit from combatant immunity, meaning they have the right under IHL to directly participate in hostilities and may not be punished or prosecuted for their participation in accordance with IHL. Third, states are responsible for the conduct of their agents, including members of their armed forces.

Members of hacker groups are usually civilians, but they may become combatants. They are therefore targetable only under certain circumstances. First, if the group is part of the armed forces of a party to a conflict, members of the group are combatants.<sup>41</sup> Membership in a state's regular armed forces is not regulated by international law, but by the state's domestic legislation, which might, for example, formally incorporate the members of a certain hacker group into the state's armed forces. Second, members of hacker groups that belong to a state, but are not formally incorporated into its armed forces, may still be combatants – and therefore liable to attack – if certain conditions are met.<sup>42</sup>

If members of hacker groups are captured by an adversary state, that gives rise to the question of their legal status in detention. As outlined above, members of a hacker group belonging to a state would be combatants and granted POW status in at least two situations: (1) if the hacker group formally constitutes part of the armed forces of the state; or (2) if the group performs a combat function and fulfils certain additional criteria.<sup>43</sup> For members of other volunteer corps (including members of organized resistance

<sup>41</sup> For example, “members of military cyber units such as the US Cyber Command, China’s People’s Liberation Army’s Strategic Support Force Network Systems Department, or Israel’s Unit 8200 would qualify as combatants during an international armed conflict.” See Kubo Mačák, “Unblurring the lines: Military cyber operations and international law”, *Journal of Cyber Policy*, Vol. 6, No. 3, 2021, p. 419.

<sup>42</sup> See, notably, Rule 4 of the ICRC’s Customary IHL Study. This requires at least a *de facto* relationship between a hacker group that meets the required organization criterion (see above) and a party to the conflict. Depending on the circumstances, this relationship may be officially declared, but may also be expressed through tacit agreement or conclusive behaviour that makes clear for which party the group is carrying out the cyber operations. See ICRC, *Interpretive Guidance*, p. 23.

<sup>43</sup> Art. 4, Third Geneva Convention; Arts 43 and 44, Additional Protocol I. As Art. 45 of Additional Protocol I states, “[a]ny person who has taken part in hostilities, who is not entitled to prisoner-of-war status and who does not benefit from more favourable treatment in accordance with the Fourth Convention shall have the right at all times to the protection of Article 75 of this Protocol”.

movements) that belong to a party to the conflict, one criterion for qualifying for POW status<sup>44</sup> is that the group must be commanded by a person responsible for their subordinates: in other words, the group must have a command structure, one that includes an internal disciplinary system capable, *inter alia*, of enforcing compliance with the rules of international law applicable in armed conflict.<sup>45</sup>

A 'command structure' does not necessarily need to follow a hierarchical design. More decentralized command structures – including those prevailing in groups that are organized virtually – may still meet the command structure requirement. The absence of a centralized command structure within the group could be compensated for, for instance, by the existence of other factors demonstrating the group's organization, such as a 'digital headquarters', group insignia, code(s) of conduct, or centralized mechanisms for recruiting new members.

Of particular importance is the ability of a command structure to impose discipline within the group, including respect for the laws and customs of war. A traditional disciplinary system is unlikely to be established by groups operating only virtually, without any physical contact between the members. However, a disciplinary system should not necessarily be understood only in the traditional military sense. Instead, what is necessary under IHL is a system that (1) sets clear rules for the conduct of members of the group and (2) is enforceable through the imposition of sanctions on the members. Some doubts exist as to whether 'informal sanctions' – also referred to as 'social sanctions' – could be considered a disciplinary system. Social sanctions may consist of the unwritten rules or customs of a group, for example, and might include penalties such as criticism or exclusion (temporary or permanent) from the group.

If members of hacker groups are not part of the state's armed forces or otherwise qualify for POW status as discussed above, they must be considered civilians protected under the Fourth Geneva Convention (if they meet the criteria of Article 4 of that Convention) and under Article 75 of Protocol I of 8 June 1977 additional to the Geneva Conventions (Additional Protocol I). However, unlike combatants, civilians are not protected from prosecution under national law for committing acts that are lawful under IHL, including through direct participation in hostilities.

## THE LEGAL STATUS OF HACKER GROUPS IN NON-INTERNATIONAL ARMED CONFLICT

Hacker groups may also be involved in – or even party to – a non-international armed conflict (NIAC), which can occur between one or more states and one or more non-state armed groups, or between such groups.

Even in NIACs, hacker groups are not usually parties to conflict. Instead, as in IACs, their members mostly operate as civilians in the context of an armed conflict. Thus, they must comply with the relevant rules of IHL and are exposed to the dangers arising from hostilities, including the loss of protection against attack, and – if captured – they risk facing prosecution for cybercrimes as defined by the adversary.<sup>46</sup>

Under certain conditions, hacker groups may become party to an NIAC, which would mean that IHL applies to their relationship with the other party to the conflict. This could be the case in at least two scenarios (further discussed below). Both scenarios require, however, that such hacker groups show a certain degree of internal organization, in addition to other elements.

<sup>44</sup> For such groups, Art. 4(2) of the Third Geneva Convention defines the following conditions for enjoying POW status: "(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war."

<sup>45</sup> Art. 4(2), Third Geneva Convention.

<sup>46</sup> See Chapter 2 above.

When considering the internal organization of hacker groups, it becomes clear that hacker groups today exist in various forms.<sup>47</sup> Some have a command structure (whether centralized or decentralized, as noted above) and meet physically. It is conceivable that such hacker groups would be organized to the degree required to become party to an NIAC. However, it is more common for hacker groups to be organized primarily or exclusively online, meaning that they have no physical infrastructure (such as a headquarters) and no physical meeting points; conduct digital activities without a formal hierarchy or command structure; and operate with no geographical boundaries. It is unlikely that such groups would meet the degree-of-organization criterion for becoming party to an armed conflict.

If a hacker group is sufficiently organized, at least two scenarios may make it party to an armed conflict.

First, an organized hacker group might be operating in the context of a pre-existing NIAC. In this situation, cyber operations by this hacker group in support of one party against another in a pre-existing conflict might make it a party to the conflict if the conditions of the ‘support-based approach’ are met.<sup>48</sup> This would require, for example, that the cyber operations of such an organized hacker group must support the collective conduct of hostilities and have a direct impact on the opposing party’s ability to carry out its military operations. In addition, the group’s operations would need to be carried out objectively in support of a party to that pre-existing conflict, in particular by pooling its military resources with that party.<sup>49</sup>

Second, hacker groups might conduct cyber operations against a state outside the context of a pre-existing armed conflict. To determine whether such operations bring about the existence of an NIAC, two criteria that reflect customary IHL must be met cumulatively: a minimum level of organization for the non-state armed group (see above), and a minimum level of intensity for the hostilities.<sup>50</sup> With regard to the required minimum level of intensity for a situation of violence to amount to an NIAC, the question arises of whether cyber operations *alone* could meet this condition – that is, without concomitant kinetic hostilities. Several states have expressed the view that NIACs between states and non-state groups that occur merely through cyber operations are possible but unlikely at present, because of the rather low level of intensity of the cyber operations conducted by most hacker groups so far.<sup>51</sup> However, this possibility should not be excluded.

During an NIAC, members of the armed forces of non-state parties, while targetable, are not protected from prosecution under national law for directly participating in hostilities.

### THE RISK FOR CIVILIAN HACKERS OF LOSING PROTECTION AGAINST ATTACK

If hackers are not part of the armed forces of a state, or a non-state party to an armed conflict, they are civilians under IHL. Civilians – including civilian hackers – are protected against direct attack unless and for such time as they directly participate in hostilities. This includes individual civilian hackers as well as hackers operating in groups that are not (part of) parties to armed conflicts. As discussed in depth in Chapter 2, civilian hackers lose this protection only if and for such time as their cyber and other digital activities qualify as ‘direct participation in hostilities’.

<sup>47</sup> See discussion in Chapter 2.

<sup>48</sup> ICRC, “How is the term ‘armed conflict’ defined in international humanitarian law?”, opinion paper, p.16; available [here](#).

<sup>49</sup> ICRC, “How is the term ‘armed conflict’ defined in international humanitarian law?”, opinion paper, p.16; available [here](#).

<sup>50</sup> International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor v. Dusko Tadić (aka ‘Dule’)*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Appeals Chamber), Case No. IT-94-1, 2 October 1995, para. 70.

<sup>51</sup> A number of states, such as [Costa Rica](#), [France](#), [Germany](#), and [Ireland](#), have maintained that the possibility of an NIAC consisting exclusively of digital activities cannot be ruled out.

## ENSURING RESPECT FOR IHL WHEN HACKER GROUPS CONDUCT CYBER OPERATIONS IN THE CONTEXT OF AN ARMED CONFLICT

Under IHL, a party must respect IHL and ensure respect for it among individuals and groups that form part of its armed forces or are “acting in fact on its instructions, or under its direction or control”.<sup>52</sup> This reflects the public international law rule according to which states incur international legal responsibility for the internationally wrongful acts of such individuals and groups.<sup>53</sup>

Accordingly, even if a hacker group is not part of the armed forces of a party to the conflict, that party is nonetheless responsible for its conduct if the group is operating under the instructions, direction or control of the party. Regarding the interpretation of the notion of ‘direction or control’, there is a long-standing debate on the level of control required for a state to incur responsibility for the acts of private actors (i.e. whether ‘effective’ or ‘overall’ control is required). In the view of the ICRC and other experts and institutions, for organized armed groups ‘overall control’ is both required and sufficient.<sup>54</sup> This means that what is required is a degree of control that goes “beyond the mere financing and equipping” of the cyber group by the state, and that also involves the state “participation in the planning and supervision of military operations”.<sup>55</sup> In contrast, the International Court of Justice, and other legal experts, require that for a wrongful act of an individual or group to qualify as being under the ‘direction or control’ of a state, the state must exercise ‘effective control’ over such an act.<sup>56</sup> Although uncertainties persist over the interpretation of the notion, it is commonly agreed that the mere financing or equipping of hacker groups, or their activities, would not be sufficient to attribute the group’s conduct to a state.

The notion of ‘instruction’ may also be relevant in the cyber context. In the view of the International Law Commission, individuals or groups can be regarded as operating under the instructions of a state if “specific instructions concerning the commission of that particular act had been issued by that State to the individual or group in question”.<sup>57</sup> Following this interpretation, a state would be responsible in situations in which it gives specific instructions to a hacker group regarding the commission of a particular cyber operation in violation of IHL.

Even when states cannot be held internationally responsible for a hacker group’s conduct, several obligations flow from their duty to *ensure* respect for IHL.<sup>58</sup> For example, as discussed in detail above (see Chapter 2), states must not encourage private persons or groups to act in violation of IHL,<sup>59</sup> irrespective of the means – online or offline – that is used to do so. Likewise, they must not aid or assist in violations of IHL. As discussed in Chapter 2 above, states also have a due diligence obligation to prevent IHL violations by civilians over whom they exercise authority and to suppress violations of IHL.

<sup>52</sup> ICRC, *Commentary on the First Geneva Convention*, 2016, paras 265–273. See also, [Rule 139](#) of the ICRC’s Customary IHL Study; Art. 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA); International Court of Justice, *Application of the Genocide Convention (Provisional Measures)*, para. 130.

<sup>53</sup> Ibid.

<sup>54</sup> “In order to attribute the acts of a military or paramilitary group to a state, it must be proved that the state wields overall control over the group, not only by equipping and financing it, but also by coordinating or helping in the general planning of its military activity.” ICTY, *The Prosecutor v. Tadić* (Appeals Chamber), Jurisdiction, para. 131.

<sup>55</sup> ICTY, *The Prosecutor v. Tadić* (Appeals Chamber), Jurisdiction, para. 273.

<sup>56</sup> ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, ICJ Reports 1986, para. 115.

<sup>57</sup> ICTY, *The Prosecutor v. Tadić* (Appeals Chamber), Jurisdiction, para. 137.

<sup>58</sup> Common Art. 1.

<sup>59</sup> Common Art. 1; [Rule 144](#) of the ICRC’s Customary IHL Study; ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, ICJ Reports 1986, para. 220.



**CHAPTER 4****IHL AND PRIVATE TECHNOLOGY COMPANIES' SERVICES AND OPERATIONS IN ARMED CONFLICT**

As private technology companies increasingly operate in contexts affected by armed conflicts – including by offering products or services to parties to conflicts – and cyber and other digital activities are increasingly part of hostilities, it is necessary to understand what implications private technology companies' operations have under IHL. These implications include, first, the protections that IHL affords to tech companies – including their employees and property – and when these protections may be lost; and second, possible IHL obligations of employees, companies, and states. The types of products and services that private technology companies provide in situations of armed conflict have significant implications in this respect. In addition, if a technology company decides to operate in the context of an armed conflict, it should give due consideration to the risks that this may pose for the company's other customers.

In general terms, several of the questions arising for tech companies – in particular the status and protection of their employees and the obligation of states to ensure respect for IHL by these actors – overlap with issues already addressed regarding IHL and individuals (Chapter 2) and hacker groups (Chapter 3) involved in armed conflicts. Thus, the discussion in this chapter focuses on additional considerations specific to private technology companies.

**IHL PROTECTION FOR THE PERSONNEL AND PROPERTY OF PRIVATE TECHNOLOGY COMPANIES**

IHL provides legal protection for the civilian personnel and property of private business entities, including technology companies.<sup>60</sup> Such protections can, however, be lost because of certain activities by a company's personnel or certain uses of its property. The practical impact of such loss of protection can be mitigated by the choices a business makes about the activities and services it offers as well as the structure or location of its assets, including its digital assets.<sup>61</sup>

Unless individual personnel are combatants (as discussed in Chapter 3), they are civilians and are protected against attack unless and for such time as they take a direct part in hostilities. The way IHL applies to civilians involved in digital activities, in the context of an armed conflict, has been covered in the preceding chapters. Thus, the following paragraphs focus on issues that have not been addressed with regard to individuals and groups.

<sup>60</sup> For a general discussion of this subject, see ICRC, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*, ICRC, Geneva, 2024; available at <https://www.icrc.org/en/publication/private-businesses-and-armed-conflict-introduction-relevant-rules-international>.

<sup>61</sup> See also discussion in Horowitz, "One click from conflict" (cited in footnote 4 above), p. 324. The author explains that another way of assessing the protection for a company is by looking at IHL's protections for 'property': "For example, distinct from the rules protecting civilian objects against attack, IHL also prohibits the destruction or seizure of the property of an adversary, unless required by imperative military necessity. The property protected is both private and public."

Considering that many private technology companies are involved in so-called defensive activities – such as providing cybersecurity services or sharing cyber-threat intelligence with a party to an armed conflict – one question that arises is whether employees who take part in these activities could be considered to be directly participating in hostilities. Under IHL, this question requires a case-by-case analysis (see Chapter 2). For example, the sharing of threat intelligence by a tech company, with the purpose of defending civilian objects during an armed conflict, would not amount to ‘direct participation in hostilities’, but sharing such intelligence for the purpose of defending a military objective might. Another challenge specific to private technology companies is related to meeting the ‘belligerent nexus criterion’ for ‘direct participation in hostilities’. For instance, if a private technology company is hired to defend the ICT system of a piece of civilian infrastructure, such as an electricity or communications provider, its staff may not know from whom they are defending that system (e.g. whether the attackers are cyber criminals or a party to an armed conflict that might consider such infrastructure a military objective).<sup>62</sup> In such circumstances, a company’s staff may be unable to assess whether their defensive activities are linked to an armed conflict, or affect the military operations of the warring parties, raising questions about whether their conduct may in these circumstances amount to ‘direct participation in hostilities’.

With regard to the development of malware and zero-day vulnerabilities, which some companies offer, one may draw an analogy with private-sector employees manufacturing and selling munitions and other military goods. Just as the manufacturing and selling of weapons is widely accepted as not qualifying as ‘direct participation in hostilities’,<sup>63</sup> the production and sale of cyber tools would similarly also not qualify. Likewise, employees of private technology companies involved in the detection of zero-day vulnerabilities and other cyber threats would not meet the threshold for ‘direct participation in hostilities’, even if such vulnerabilities are shared with a belligerent.

As noted above, whenever there is any doubt about whether they directly participate in hostilities, civilian employees of private companies are presumed to remain protected against direct attack.

Private technology companies’ property consists primarily of their infrastructure. In the ICT context, this means the physical and software-based assets necessary to deliver the company’s products and services. Unless military in nature, such infrastructure must be regarded as civilian objects under IHL. Under the principle of distinction, IHL prohibits attacks directed against civilian objects, but does not prohibit attacks against military objectives. As Additional Protocol I provides, “[i]n so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage”.<sup>64</sup> Every object that is not a military objective is a civilian object under IHL.<sup>65</sup>

How to assess when a private technology company’s asset has become a military objective is therefore an important question. This must be done by assessing the two-pronged customary test described in the preceding paragraph. In today’s armed conflicts, it may well be the case that certain assets are used by belligerents, or by technology companies and their employees, in ways that make an effective contribution to military action. When addressing whether thereby they become military objectives, it must be carefully considered whether attacking such assets would, in fact, offer a definite military advantage. In this respect, it is important to consider the high level of redundancy in the ICT environment – meaning that one of its characteristics is the ability to immediately re-route data traffic (for example to maintain connectivity).<sup>66</sup> This inbuilt resilience may render it challenging for militaries to establish that a target’s destruction or neutralization would offer a definite military advantage as required by the definition of ‘military objective’. If such a definite advantage does not exist, private technology companies’ assets remain civilian objects and must not be attacked.

<sup>62</sup> For a discussion of the issues this poses for the requirement of ‘belligerent nexus’, see Mačák, “Will the centre hold?” (cited in footnote 4 above), pp. 976–977; Horowitz, “One click from conflict” (cited in footnote 4 above), pp. 320–321.

<sup>63</sup> See also ICRC, *Interpretive Guidance*, p. 53.

<sup>64</sup> Art. 52(2), Additional Protocol I; Rule 8, Customary IHL Study.

<sup>65</sup> Art. 50, Additional Protocol I; Rule 5, Customary IHL Study.

<sup>66</sup> ICRC, *Commentary on the First Geneva Convention*, 2016, p. 42.

## ENSURING THAT PRIVATE TECHNOLOGY COMPANIES' OPERATIONS RESPECT IHL

In principle, IHL does not impose legal obligations directly on private technology companies.<sup>67</sup> It applies to the activities of a technology company in so far as it directly applies to acts of the company's personnel (see Chapter 2 above). In addition, national laws can impose obligations on both tech companies and on their personnel, or provide for civil liability or regulatory or criminal penalties in relation to IHL.

In order to ensure that private companies' personnel do not violate IHL, and as discussed in particular in Chapter 1, states have a due diligence obligation to ensure respect for IHL among civilians over whom they exercise authority. Depending on the degree of influence they have over private technology companies, states may adopt various measures for ensuring that such companies and their employees respect IHL.<sup>68</sup> This should involve a combination of measures to prevent violations of IHL and measures to respond to violations if they do occur. More generally, states often regulate the activities of private businesses through administrative regulatory regimes based on their national laws: adopting and enforcing regulatory requirements in relation to IHL, when companies operate in situations of armed conflict, can be one such measure. In addition, states must investigate allegations of serious violations of IHL – such as war crimes – and criminally prosecute perpetrators.<sup>69</sup> In this regard, when the legal system of a state provides for the possibility of criminal responsibility for corporate entities, the state should ensure that such legislation also applies to technology companies.

In addition, technology companies should explore possibilities for practical measures to minimize risks to their employees, property, and the customers of their products and services.<sup>70</sup> This is particularly important, given the risk of harm to civilians if private technology companies become involved in an armed conflict. Good practices in this respect should include offering IHL training to employees who carry out cyber operations or other activities related to armed conflict, so that they understand and comply with the applicable IHL rules. Companies should also assess and mitigate the risks their activities expose employees and customers to.

Another important measure private technology companies can take involves managing their assets and services in ways that minimize the risk of incidental harm to civilians. This might include finding solutions to digitally segregate assets used by a company's civilian customers from those used by its military customers. Several challenges exist in this respect: one is that it may not always be technically feasible to segregate an asset or network; and even when that is feasible, companies may resist such solutions because of the expenditure involved. While certain segregation measures can be taken once a conflict breaks out, others may need to be put in place *before* an armed conflict starts. Further discussion and study would also be required to determine whether and to what extent segregation, or the use of segregated networks only for military purposes, are part of a conflict party's obligation to take all feasible precautions against the effect of attacks.<sup>71</sup>

<sup>67</sup> By definition, an IAC is a conflict between states. Therefore, private companies cannot themselves become party to an IAC. However, company staff could, in principle, form part of a state's armed forces, *de jure* or *de facto*, as discussed above with regard to hacker groups. Moreover, a private technology company could, in principle, become party to an NIAC if it meets the established legal criteria noted above for groups. See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2015, pp. 21–22; available at <https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts>.

<sup>68</sup> Common Art. 1. States have an obligation to exercise due diligence to prevent and repress breaches of IHL by the population “over which they exercise authority, i.e. also to private persons whose conduct is not attributable to the State”: ICRC, *Commentary on the Third Geneva Convention*, 2020, para. 183.

<sup>69</sup> For more on this, see the discussion in Chapter 2.

<sup>70</sup> Horowitz, “One click from conflict” (cited in footnote 4 above), pp. 334–337.

<sup>71</sup> Art. 58, Additional Protocol I; Rule 158, ICRC Customary IHL Study.

# THE NEED FOR FURTHER STUDY AND DIALOGUE

As ‘total’ or ‘comprehensive’ defence strategies continue to be reviewed and redrawn, the current trend of involving civilians in activities closely linked to hostilities is likely to grow. The digitalization of our societies and of contemporary armed conflicts contributes to the acceleration of this trend. Civilian involvement in armed conflicts through digital means raises important legal questions about the protection of civilians and their obligations under IHL. While the legal research and consultations with experts underlying this report focused on cyber- or digital-specific issues, they are also relevant for studying similar legal questions that arise in connection with civilian involvement in any other activities related to armed conflict.

Civilians involved in cyber operations during armed conflict must respect IHL. Furthermore, parties to armed conflict must take action to prevent or otherwise minimize the harmful effects of civilian involvement in armed conflict. This includes engagement with civilian populations, including hacker groups and technology companies, to ensure that IHL is respected at all times. Some of the issues discussed in this report have been addressed by states and members of the International Red Cross and Red Crescent Movement in Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, titled “Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict”. This report presents a detailed explanation of these matters from a legal perspective. Discussion of some of these issues has also begun to take place (and will continue into 2026) in the ICT Workstream of the Global Initiative to Galvanize Political Commitment to International Humanitarian Law. It is hoped that the report will help inform and enrich those deliberations.

It is also hoped that this report will contribute to a better understanding of the application of IHL in an ICT environment; clarify legal questions; and, ultimately, prevent harm. The report identifies not only those areas in which IHL seems clear, but also issues that demand further attention. It sets out practices aimed at ensuring respect for IHL, with the objective of preventing or minimizing harm to civilian populations. Importantly, the report also confirms the need to continue conducting research and dialogue in this area, in particular by states, international organizations, the private technology sector, academia, and civil society.

# EXPERTS WHO PARTICIPATED IN THE EXPERTS' MEETING RELATED TO THIS REPORT

- Mr Benjamin Ang, Centre of Excellence for National Security, Nanyang Technological University, Singapore
- Prof. Martha Bradley, University of Johannesburg, Johannesburg, South Africa
- Prof. Russell Buchan, University of Reading, Reading, United Kingdom
- Ms Kaja Ciglic, Senior Director, Digital Diplomacy at Microsoft, Ljubljana, Slovenia
- Prof. Gary Corn, American University Washington College of Law, Washington DC, United States of America
- Ms Lindsay Freeman, University of California, Berkeley, United States of America
- Dr Aude Gery, GEODE Université de Paris 8, Paris, France
- Dr Heather Harrison Dinniss, Swedish Defence University, Stockholm, Sweden
- Prof. Zhixiong Huang, Wuhan University School of Law, Wuhan, China
- Dr Pia Husch, Royal United Services Institute (RUSI), London, United Kingdom
- Dr Andraz Kastelic, United Nations Institute for Disarmament Research (UNIDIR), Geneva, Switzerland
- Prof. Kubo Mačák, University of Exeter, Exeter, United Kingdom
- Prof. Mariana Salazar, Universidad Iberoamericana, Mexico City, Mexico
- Mr Michael Siegrist, Swiss Federal Department of Foreign Affairs, Bern, Switzerland
- Mr Stefan Soesanto, Center for Security Studies at ETH Zurich, Zurich, Switzerland
- Dr Papawadee Tanodomdej, Chulalongkorn University, Bangkok, Thailand
- Prof. Nicholas Tsagourias, University of Sheffield, Sheffield, United Kingdom
- Dr Tsvetelina Van Benthem, Oxford Institute for Ethics, Law and Armed Conflict, Oxford, United Kingdom

## ICRC AND GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS

- Pierrick Devidal, Policy Adviser, ICRC
- Jonathan Horowitz, Legal Adviser, ICRC Delegation for the USA and Canada
- Joelle Rizk, Digital Risks Adviser, ICRC
- Ruben Stewart, Technology in Warfare Adviser, ICRC











The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles.

People know they can count on the ICRC to carry out a range of life-saving activities in conflict zones and to work closely with the communities there to understand and meet their needs. The organization's experience and expertise enables it to respond quickly and effectively, without taking sides.

 [www.icrc.org](http://www.icrc.org)  
 [facebook.com/icrc](https://facebook.com/icrc)  
 [x.com/icrc](https://x.com/icrc)  
 [instagram.com/icrc](https://instagram.com/icrc)



ICRC

International Committee of the Red Cross  
19, avenue de la Paix  
1202 Geneva, Switzerland  
T +41 22 734 60 01  
[shop.icrc.org](http://shop.icrc.org)  
© ICRC, October 2025