University of Exeter

ECIL
EXETER CENTRE FOR INTERNATIONAL LAW

Protecting civilians from harm caused by cyber operations during armed conflicts

Kubo Mačák and Florentina Pircher

Forthcoming in Robert Heinsch and Jelena Plamenac (eds), *Research Handbook on Victims under International Law* (Edward Elgar 2026)

Exeter Centre for International Law

Working Paper Series

2025/1

The **Exeter Centre for International Law** builds on a long and distinguished tradition of international legal scholarship at Exeter Law School. The Centre's mission is to provide an intellectual environment for the study and development of international law and to stimulate discussion and collaboration in response to the most pressing challenges facing the international community. As part of this mission, the Centre publishes the present Working Paper Series.

Exeter Centre for International Law
Exeter Law School, Amory Building
Rennes Drive, Exeter, EX4 4RJ, United Kingdom

http://www.exeter.ac.uk/ecil
@ExeterCIL

Cite as Kubo Mačák and Florentina Pircher, "Protecting civilians from harm caused by cyber operations during armed conflicts", ECIL Working Paper 2025/1, forthcoming in Robert Heinsch and Jelena Plamenac (eds), *Research Handbook on Victims under International Law* (Edward Elgar 2026).

Protecting civilians from harm caused by cyber operations during armed conflicts

Kubo Mačák and Florentina Pircher

Abstract

As warfare increasingly spreads to the digital domain, civilians face novel and profound risks. Cyber operations during armed conflicts threaten essential services, compromise civilian infrastructure, and blur the lines between civilian and military roles. This chapter examines how international law, and particularly international humanitarian law (IHL), protects civilian populations and infrastructure from victimization by cyber means. Anchored in a detailed typology of harm posed by cyber operations to civilians, the analysis begins by exploring how peacetime legal protections can mitigate cyber-enabled harm in future armed conflicts. It then examines the legal framework governing cyber operations during armed conflicts, focussing on the IHL principles of distinction, proportionality, and precautions. Finally, it considers the role of accountability mechanisms, including international criminal law, in responding to cyber-enabled violations of IHL and delivering justice to victims. The chapter emphasizes the need for States to clarify their legal positions on the application of international law to cyber activities, adopt specific mitigating measures in both peacetime and armed conflict, and foster international co-operation to ensure robust civilian protection in the digital age.

Contents

I. Introduction

The protection of civilians lies at the heart of international humanitarian law (IHL), which seeks to shield those not participating in hostilities from the effects of armed conflict, safeguarding their safety and dignity. Yet, as warfare increasingly spreads to the digital domain, civilians face novel and profound risks. Cyber operations during armed conflicts threaten essential services, compromise civilian infrastructure, and blur the lines between civilian and military roles. These developments necessitate a thorough assessment of how international law safeguards victims of armed conflicts and addresses the vulnerabilities arising in the digital age.

Civilians harmed by cyber operations may endure a wide array of negative impacts, ranging from physical destruction and systemic disruptions to psychological trauma and economic loss. This chapter explores the ways in which international law, and particularly IHL, seeks to protect civilian populations and infrastructure from such harms. It also considers the role of accountability mechanisms under international criminal law in providing justice for victims and deterring future violations.

The analysis is presented in four interrelated steps. First, the chapter maps the specific forms of harm posed by cyber operations to civilians and civilian infrastructure during armed conflicts, organizing these risks into five overarching categories (section II). Second, it explores the peacetime legal protections established under international law, highlighting how adherence to these safeguards can mitigate victimisation of civilians in future armed conflicts (section III). Third, it evaluates the legal framework applicable once an armed conflict is underway, with a specific focus on the principles of distinction, proportionality, and precautions, and their application to cyber operations (section IV). Finally, it considers the role of accountability mechanisms, including international criminal law, in addressing cyber-enabled violations of IHL and securing justice for victims (section V).

By addressing these practical and legal dimensions, the chapter underscores the enduring relevance of IHL and the broader international legal framework in protecting civilians and civilian infrastructure from cyber harm. It identifies key strengths and areas for further development to meet the challenges of modern conflicts while placing victims at the centre of efforts to address the humanitarian impact of cyber warfare.

II. Setting the scene: Harm posed by cyber operations to civilians during armed conflicts

II. 1. Growing global acknowledgment of the risks of cyber harm

The first quarter of the twenty-first century has witnessed unprecedented advancements in information and communication technologies (ICTs). Modern societies have developed a digital layer that underpins many aspects of our daily lives, from personal relationships to business transactions and public governance. While digitalization and growing interconnectivity have brought numerous benefits and opportunities to many, increased dependency on ICTs also has also introduced new vulnerabilities to victimisation.

These tensions become particularly acute in situations of armed conflict. On the one hand, digital technologies can enhance protections for affected populations. Civilians may use smartphones to access potentially life-saving information, such as the locations of shelters or aid

distribution points.[1] Armed actors, too, can harness digital tools to reduce harm, for example, by employing technologies for minefield mapping to safeguard civilians and military personnel alike.[2]

On the other hand, cyber operations during armed conflict can inflict significant harm. Cyber capabilities may be used to trigger, alter, or otherwise manipulate processes controlled by computer systems, or to tamper with the data stored and processed by such systems. When these processes and datasets support or enable essential civilian services or the delivery of humanitarian aid, their disruption or compromise can result in substantial harm to civilian populations.[3]

This much is now recognized by the international community. In 2021, States acknowledged by consensus that cyber operations, like any other means and methods of warfare, can seriously affect critical civilian infrastructure and result in 'devastating … humanitarian consequences'.[4] More recently, in a resolution adopted by consensus at the 2024 International Conference of the Red Cross and Red Crescent, States agreed on a detailed catalogue of the risks and dangers posed by the use of ICTs in armed conflict.[5] This growing recognition highlights the importance of examining the scope and types of these harmful consequences as well as the extent to which existing legal frameworks address them.

II. 2. Mapping the harm from cyber operations during armed conflict

This chapter draws on a recent definition of harm proposed by the Cyber Peace Institute, which conceptualizes harm as '[a] negative impact on the victim or victims' physical, psychological, social, economic well-being, their physical security, their economic security, or on the environment'.[6] Cyber operations can result in one or more of these types of negative effects. For example, cyber operations targeting industrial control systems, such as those used in water treatment facilities, can cause devastating physical effects, compromise the security and well-being of downstream populations, and pollute the surrounding environment.[7]

---

[1] See, eg, Mats Granryd, 'Five Ways Mobile Technology Can Help in Humanitarian Emergencies' (World Economic Forum, 22 August 2017) <https://www.weforum.org/stories/2017/08/mobile-technology-humanitarian-crisis/> accessed 31 January 2025.

[2] See, eg, Roman Horbyk, '"The War Phone": Mobile Communication on the Frontline in Eastern Ukraine' (2022) 3 *Digital War* 9, 15 and 23.

[3] See, generally, ICRC, *The Potential Human Cost of Cyber Operations*, 2019, <https://www.icrc.org/en/document/potential-human-cost-cyber-operations> accessed 31 January 2025.

[4] UN General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/75/816 (18 March 2021) (*OEWG report*) para 16. The report was later endorsed by a UNGA resolution also adopted by consensus: see UN General Assembly, *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*, UN Doc 76/19 (8 December 2021) para 1.

[5] 34th International Conference of the Red Cross and Red Crescent, *Resolution II: Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of ICT Activities During Armed Conflict*, 34IC/24/R2 (31 October 2024), preambular paras 7–14. For an analysis, see Kubo Mačák, 'The First Humanitarian ICT Resolution: Ambitions and Limitations', *EJIL:Talk!* (25 November 2024) <https://www.ejiltalk.org/the-first-humanitarian-ict-resolution-ambitions-and-limitations/> accessed 31 January 2025.

[6] Cyber Peace Institute, *Expert Meeting: Towards a Methodology for Defining Harms in Cyberspace* (December 2023) <https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Expert-Meeting-Harms-Methodology.pdf> accessed 31 January 2025, 12.

[7] Sergio Caltagirone, 'Industrial Cyber Attacks: A Humanitarian Crisis in the Making', *Humanitarian Law and Policy Blog* (3 December 2019) <https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/> accessed 31 January 2025.

Broadly speaking, these forms of harm can be clustered into five thematic categories. First, cyber operations may cause **direct harm to civilians, civilian systems and services**. For instance, cyber operations targeting the power grid or healthcare sector can interrupt access to electricity or critical medical care, endangering civilian lives and well-being. Similarly, cyber operations can cause physical damage to civilian infrastructure, as seen in the reported operations against a German steel mill in 2014, illustrating the destructive potential of such activities.[8]

Second, the growing involvement of civilians and private companies in digital activities during armed conflicts – also known as the **civilianization of the digital battlefield**[9] – erodes the protective distinction between armed forces and the civilian population, increasing the risk of harm to individuals. In ongoing conflicts, civilians have contributed to the military intelligence collection using smartphone apps, taken up roles in cyber defence in support of armed actors, and even engaged in offensive cyber operations against enemy targets.[10] Such activities expose civilians to serious risks, including being targeted, detained, or having their property seized or destroyed.[11] A related issue is the military use of civilian cyber infrastructure, such as communication networks or undersea cables, which further endangers civilians reliant on such infrastructure.[12]

Third, cyber and digital activities during armed conflict can inflict significant **non-tangible psychological, social, and economic harm**. This includes psychological effects such as fear or trauma, which research has shown to be comparable to those caused by conventional political violence or terrorism.[13] It also includes societal disruption and erosion of trust due to the spread of misinformation and disinformation via digital means. Furthermore, economic harm, such as financial losses stemming from malicious cyber operations, also falls within this category.[14]

Fourth, cyber capabilities used during armed conflict present **systemic and interconnected risks**. These include ripple effects and potential for cascading failures stemming from the interconnectivity of ICTs and the proliferation of cyber tools. Incidents such as *WannaCry*, *NotPetya*, or *Triton* have demonstrated how malware can spread globally in an instant not only threaten specific civilian systems but can also easily reach and impact any number of critical civilian infrastructures around the world.[15] Moreover, once deployed, cyber tools can be reverse-engineered and repurposed by other, potentially less scrupulous actors.[16]

---

[8] Samuele De Tomas Colatin, 'Steel mill in Germany (2014)', *Cyber Law Toolkit* (9 June 2021) <https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_(2014)>.

[9] Kubo Mačák and Mauro Vignati, 'Civilianization of Digital Operations: A Risky Trend', *Lawfare* (5 April 2023) <https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend> accessed 31 January 2025.

[10] Kubo Mačák, 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield' (2023) 105(923) International Review of the Red Cross 965, 968–969.

[11] Joelle Rizk and Sean Cordey, 'What we don't understand about digital risks in armed conflict and what to do about it', *Humanitarian Law and Policy Blog* (27 July 2023) <https://blogs.icrc.org/law-and-policy/2023/07/27/digital-risks-in-armed-conflict/> accessed 31 January 2025.

[12] 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' (2020) 102(913) *International Review of the Red Cross* 287, 320.

[13] Ryan Shandler, Michael L Gross, and Daphna Canetti, 'Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis' (2023) 8(1) *Journal of Global Security Studies* 1, 15.

[14] Pia Hüsch and Henning Lahmann, *Societal Risks and Potential Humanitarian Impact of Cyber Operations* (Geneva Academy, June 2022) 11.

[15] Gisel, Rodenhäuser and Dörmann (n 12) 294.

[16] ICRC, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts* (2021) 19.

Finally, the use of military cyber capabilities carries significant **risks of escalation**. A key driver of this risk is the potential for misperception regarding the intentions of the acting party. For instance, a defending party may detect a hostile presence within its networks but struggle to discern whether the intrusion is intended as mere intelligence gathering or as preparation for disruptive or destructive actions.[17] This ambiguity can lead to miscalculated responses and inadvertent escalation of conflict.[18] Additionally, the proliferation of cyber tools heightens the risk of escalation by enabling malicious actors to deploy them in ways that exacerbate tensions.[19] The possibility of 'false flag operations', where hackers disguise themselves as agents of another State, further increases the risk of retaliatory actions against the wrong party.[20]

This panorama of risks associated with the use of cyber and digital means during armed conflicts underscores the critical importance of understanding the protections that international law affords to civilians and civilian infrastructure. In this regard, IHL serves as a 'legal firewall', offering safeguards some of which apply already in peacetime while others are triggered once an armed conflict is underway.[21] These protections are further reinforced by other branches of international law, including international criminal law, which aims to ensure accountability and enforcement for violations. The following sections analyse these legal frameworks and how they collectively work to protect civilians and civilian infrastructure from the harm posed by cyber operations.

III. Peacetime protections and safeguards against cyber harm

III. 1. Applicable bodies of international law

Cyberspace has become inextricably linked to our daily lives, infrastructure, and governance. Consequently, the international legal rules established to regulate the physical world have been recognized as equally applicable to uses of ICTs.

Among these rules, the least controversial are those enshrined in the UN Charter, which have been explicitly reaffirmed in several consensus reports by groups of governmental experts[22] and subsequently endorsed by the entire UN General Assembly.[23] Accordingly, there is no doubt that the rules governing the use of force – also known as the *jus ad bellum* – codified in the Charter,

---

[17] Gisel, Rodenhäuser and Dörmann (n 12) 296.

[18] ICRC, *Avoiding Civilian Harm* (n 16) 12.

[19] Winnona DeSombre et al, *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service* (Atlantic Council, 2021) <https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf> accessed 31 January 2025.

[20] *The Council of Advisers' Report on The Application of The Rome Statute of The International Criminal Court to Cyberwarfare*, prepared by the Permanent Mission of Liechtenstein to the United Nations (2021) 30; Petr Stejskal and Martin Faix, 'Scenario 21: Misattribution caused by deception' Cyber Law Toolkit (3 February 2023) <https://cyberlaw.ccdcoe.org/wiki/Scenario_21:_Misattribution_caused_by_deception> accessed 31 January 2025.

[21] Peter Maurer, 'Developing a New Humanitarian Response in the Area of Cyberspace', Samir Saran (ed), *Our Common Digital Future* (ORF 2017) 33.

[22] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 (24 June 2013) para 19; UN General Assembly, *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 24; UN General Assembly, *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) (*GGE report 2021*) para 69.

[23] See, eg, UN General Assembly, Res 68/243 (27 December 2013) UN Doc A/RES/68/243.

constrain States in their uses of ICTs inasmuch as they do in the physical space. States are therefore obliged to take measures to ensure that cyberspace does not become a source of armed conflict. In particular, States should adopt policies and practices to enhance clarity, predictability, and stability in cyberspace, thereby mitigating systemic and escalation risks and protecting civilians.

It is also widely accepted that international human rights law applies online just as it does offline. This means that States must respect, protect, and fulfil human rights in cyberspace.[24] States are accountable for human rights violations attributable to them, primarily under treaties like the International Covenant on Civil and Political Rights[25] and the International Covenant on Economic, Social and Cultural Rights,[26] alongside regional instruments such as the European Convention on Human Rights.[27] Furthermore, States may bear responsibility for failing to protect individuals from human rights abuses perpetrated by non-State actors within their territory or jurisdiction.[28] These protections safeguard individuals from cyber harm during peacetime, and it is generally accepted that their applicability extends also to situations of armed conflict.[29]

The focus of this chapter, however, is on IHL. There is now broad agreement among States that IHL applies to cyber operations during armed conflicts and that affirming this applicability does not legitimize conflict or encourage militarization.[30] Furthermore, IHL imposes certain obligations that States must fulfil even during peacetime to ensure respect for IHL in the event of armed conflict. These obligations include disseminating and training on IHL, adopting implementing domestic legislation, reviewing the legality of new weapons, means, and methods of warfare, and taking measures to protect civilians and civilian infrastructure against the effects of attacks.[31] These rules, to which we turn in the following subsection, form an essential foundation for safeguarding civilians in the digital age and mitigating the unique risks posed by cyber operations.

III. 2. IHL obligations applicable in peacetime

A cornerstone obligation of IHL is the duty to respect and ensure respect for its provisions.[32] This obligation applies both during armed conflict and in peacetime. The obligation to ensure

---

[24] See, eg, UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, UN Doc A/HRC/RES/32/13 (1 July 2016) para 1.

[25] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

[26] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3.

[27] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS 5.

[28] See, eg, *Velásquez Rodríguez v Honduras* (Merits) IACtHR Series C No 4 (29 July 1988) para 177.

[29] For a recent overview, see Kubo Mačák, 'The Role of International Human Rights Law in the Interpretation of the Fourth Geneva Convention' (2022) 52 *Israel Yearbook on Human Rights* 219, 227–228, concluding that 'most IHRL treaty rules may apply in extraterritorial settings during armed conflicts, provided that the State in question exercises its jurisdiction over individuals there'.

[30] See *GGE report 2021* (n 22) para 71(f).

[31] Kubo Mačák, 'Unblurring the Lines: Military Cyber Operations and International Law' (2021) 6(3) *Journal of Cyber Policy* 411, 423 fn 2.

[32] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (GC I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (GC II); Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (GC III); Geneva

respect extends to actors whose conduct is not attributable to the State in question,[33] such as hackers operating independently from the concerned State's territory. Moreover, the prevailing view is that this obligation also has an external dimension, requiring States to take feasible measures to promote the universal respect for IHL, including by influencing the behaviour of other States and belligerents.[34]

Dissemination of IHL is another critical obligation that applies in peacetime. States must disseminate IHL as widely as possible, including by instructing their armed forces on how to comply with IHL.[35] For States whose armed forces are or may become engaged in cyber operations, this in our view includes clarifying their positions on how IHL applies to such activities. The obligation to disseminate IHL also extends to non-military audiences, such as private technology companies and the general population, to raise awareness of the legal and practical risks associated with involvement in digital activities during armed conflict.[36]

States must also prevent and repress the abuse of protective emblems, such as the red cross, red crescent, and red crystal.[37] Although the misuse of these emblems in cyberspace has so far been limited, the special protection that IHL affords to medical and humanitarian facilities remains fully applicable.[38] For this reason, the ICRC has initiated a process of digitalizing these emblems, identifying ways to safeguard them in cyberspace.[39] This initiative offers promising avenues for protecting civilian systems and services from harm, and it has recently received additional support

---

Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (GC IV), common Art 1; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (AP I), Art 1(1); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law: Volume I, Rules* (ICRC and CUP 2005) (*ICRC CIHL Study*) Rules 139 and 144; 26th International Conference of the Red Cross and Red Crescent, *Resolution 1: International Humanitarian Law – From Law to Action*, 26IC/95/R1 (3 December 1995) para 2. Ensuring the respect for IHL also requires the suppression of breaches of IHL, related to the States' obligation to establish universal jurisdiction for grave breaches of the Geneva Conventions and their obligation to investigate war crimes, which is further discussed in section V of this chapter.

[33] ICRC, *Commentary on the Third Geneva Convention* (CUP 2020) (*Commentary on GC III*), commentary on common Article 1, para 183.

[34] *ICRC CIHL Study* (n 32) Rule 144; *Commentary on GC III* (n 33), commentary on common Article 1, para 186; 34th International Conference of the Red Cross and Red Crescent, *Joint Statement of the Kingdom of Spain and the Spanish Red Cross* (31 October 2024) (made jointly on behalf of 74 national societies and 66 States) ('This obligation … requires States to comply actively with IHL, but also to take, to the extent possible, the necessary measures to ensure that other States and individuals bring their conduct into conformity with IHL.').

[35] GC I-IV, Arts 47/48/127/144; AP I, Art 83; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (AP II), Art 19.

[36] See *Resolution II* (2024) (n 5), operative paras 9 and 11; see also Jonathan Horowitz, 'One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict' (2024) 24(2) Chicago Journal of International Law 305, 335.

[37] See GC I, Arts 53–54 First Geneva Convention. See also *Commentary on GC III* (n 33), commentary on common Article 1, para 179.

[38] Jeffrey Biller, 'The Misuse of Protected Indicators in Cyberspace: Defending a Core Aspect of International Humanitarian Law' in Henry Rõigas et al (eds), *2017 9th International Conference on Cyber Conflict: Defending the Core* (CCDCOE 2017).

[39] ICRC, *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions* (ICRC 2022); see also Samit D'Cunha, 'Conceive, standardize, integrate: the past, present, and future of adopting distinctive emblems and signs under IHL' *Humanitarian Law and Policy Blog* (12 September 2024) <https://blogs.icrc.org/law-and-policy/2024/09/12/conceive-standardize-integrate-the-past-present-and-future-of-adopting-distinctive-emblems-and-signs-under-ihl/> accessed 31 January 2025.

through the resolution adopted at the 2024 International Conference of the Red Cross and Red Crescent.[40]

Another critical obligation, codified in Additional Protocol I, is the obligation to review the legality of new weapons, means, and methods of warfare.[41] This obligation requires States to ensure that the weapons and tactics employed in prospective fighting will be capable of complying with IHL. Realistically, respect for this provision necessitates that measures be taken already in peacetime, such as the establishment of a reviewing authority and the review of weapons upon acquisition or development.[42]

When cyber capabilities qualify as weapons, means, or methods of warfare, they come within the purview of this obligation. This has been acknowledged by a growing number of States – including Australia, Brazil, Canada, Costa Rica, or Switzerland[43] – and some have developed internal guidance on how to conduct these reviews in the cyber context.[44] Effective implementation of these reviews depends on States developing clear positions on key issues, such as which cyber capabilities constitute weapons, means, or methods of warfare, and which cyber operations qualify as attacks under IHL.[45] Moreover, these reviews must consider the interconnected and systemic risks unique to cyber operations, ensuring compliance with IHL in the intended operating environment.[46]

Finally, States must put in place measures to protect civilians and civilian objects against the dangers resulting from military operations, commonly referred to as 'passive precautions'.[47] This obligation undoubtedly applies in the cyber context, as expressly recognized by States such as Costa Rica[48] and France.[49] Some of these measures may have to be implemented already in peacetime. In particular, States should build strong cyber resilience cultures at the societal level, raise public awareness of cyber risks, segregate civilian and military cyber networks and infrastructure, set up systems for the detection of cyber vulnerabilities, and engage with private owners of relevant infrastructure.[50] These measures are essential not only to prevent harm to civilian systems and

[40] *Resolution II* (2024) (n 5), operative para 12.

[41] AP I, Art 36.

[42] ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (ICRC 2006) 23–25.

[43] See further 'Legal Review of Cyber Weapons, Means and Methods of Warfare' *Cyber Law Toolkit* (20 May 2024). <https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare> accessed 31 January 2025.

[44] See, eg, Australia, *The Australian Article 36 Review Process*, UN Doc CCW/GGE.2/2018/WP.6 (30 August 2018) fn 6 (confirming that 'computer systems designed to attack enemy computer systems' are subject to legal review); United Kingdom, Ministry of Defence, *UK Weapon Reviews* (March 2016); US Department of Air Force, *Legal Reviews of Weapons and Cyber Capabilities*, Instruction 51-402 (27 July 2011).

[45] Vincent Boulanin and Maaike Verbruggen, *Article 36 Reviews: Dealing with the Challenges posed by Emerging Technologies* (SIPRI 2017) 10 and 13; see also ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper* (November 2019) (*ICRC position paper*) 9.

[46] Boulanin and Verbruggen (n 45) 4.

[47] AP I, Art 58(c).

[48] Ministry of Foreign Affairs of Costa Rica, *Costa Rica's Position on the Application of International Law in Cyberspace* (21 July 2023) (National position of Costa Rica) para 54.

[49] Ministry of Defense of France, *International Law Applied to Operations in Cyberspace* (9 September 2019) (National position of France) 16.

[50] ICRC, *Avoiding Civilian Harm* (n 16) 27

services but also to address the risks posed by the civilianization of the battlefield and the interconnected nature of ICTs.

IV. Protections to be upheld by parties to armed conflicts

As noted earlier, there is a broad agreement today that IHL governs cyber operations during armed conflict. Any conflict-related use of ICTs by States or other belligerents must therefore comply with the principles and rules of IHL.[51] IHL seeks to protect those that are not, or are no longer, engaged in hostilities and imposes strict rules on how hostilities may be conducted. While the general applicability of IHL to the cyber context is now relatively uncontroversial, significant questions remain about *how* its principles and rules apply to the specific nature of cyber operations.

To begin with, for IHL to apply there must be an armed conflict, either international (between States) or non-international (involving one or more armed groups). In theory, a cyber operation could, by itself, trigger the existence of an armed conflict where none previously existed. Given that cyber operations can have effects as destructive as, or even more destructive than, kinetic attacks, there is little reason to argue otherwise in the case of international armed conflicts. Such conflicts are triggered by any use of force by one State against another.[52]

For non-international armed conflicts, however, the situation is more complex. These conflicts come into existence only once a certain threshold of intensity of violence has been reached.[53] While it remains unsettled in general whether cyber operations – particularly those without kinetic effects –can meet this threshold,[54] several States and the African Union have affirmed that, at least in theory, cyber operations could indeed trigger a non-international armed conflict.[55] The absence of consensus on this issue reflects the broader challenge of interpreting IHL principles in the evolving context of cyber warfare.

Once an armed conflict has come into existence, whether by cyber means or otherwise, IHL governs all military operations carried out in connection with that conflict, including cyber operations. Central to these rules is the conduct of hostilities framework, which provides detailed protections for civilians and civilian objects. This framework is primarily concerned with regulating attacks and imposes strict obligations on parties to a conflict to ensure that harm to civilians is minimized. Whether a cyber operation qualifies as an attack under IHL is therefore a crucial threshold question, as the key principles of distinction, proportionality, and precautions largely hinge on this determination. The following subsections examine these issues in turn.

---

[51] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflict: Building a culture of compliance for IHL to protect humanity in today's and future conflicts* (September 2024) (*Challenges Report*) 48–49.

[52] ICTY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-A (2 October 1995) para 70.

[53] See, eg, ICTY, *Prosecutor v Limaj* (Trial Judgment) ICTY-03-66-T (30 November 2005) para 84; *Prosecutor v Boškoski and Tarčulovski* (Trial Judgment) ICTY-04-82-T (10 July 2008) para 175.

[54] *Commentary on GC III* (n 33), commentary on common Article 3, para 471; *Council of Advisers' Report* (n 20) 33–36.

[55] See, in particular, Austria, *Austrian Position on Cyber Activities and International Law* (April 2024) (National position of Austria) 16; National position of Costa Rica (n 48) para 43; National position of France (n 49) 12; Federal Government of Germany, *On the Application of International Law in Cyberspace: Position Paper* (March 2021) (National position of Germany) 7; Irish Department of Foreign Affairs, *Position Paper on the Application of International Law in Cyberspace* (6 July 2023) (National position of Ireland) 7; see also African Union, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* (29 January 2024) para 48.

IV. 1. The threshold question: Cyber operations as 'attacks' under IHL

Article 49(1) of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. In other words, an attack involves an operation causing violent effects.[56] Similarly, the Tallinn Manual 2.0 has defined a cyber attack as a 'cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.'[57] Several States, as well as the ICRC, have taken the view that harm caused by the foreseeable direct as well as indirect effects of an operation should also be considered when determining the existence of damage.[58]

From the outset, there should be no doubt that cyber operations can produce violent effects, such as death, damage, or destruction (see section II above). Whether a furnace in a steel mill – to return to a previously mentioned example – is damaged through kinetic force or a cyber operation, the resulting effects can be equally destructive and violent.

However, most cyber operations do not result in kinetic effects. Instead, their main consequence is often the disabling (also referred to as the loss of functionality) of ICT systems or infrastructure without physical damage. Among the States that have expressed views on the application of IHL to cyberspace, some consider operations without physical effects to fall outside of the definition of 'attack'.[59] Proponents of this view reason that the rules on targeting are intended to regulate destructive effects similar to those of kinetic warfare.[60]

A slightly more nuanced perspective is reflected in the majority view among the Tallinn Manual 2.0 experts. According to this view, the loss of functionality can constitute the kind of damage required for a cyber operation to amount to an attack, provided that repairing the damaged system necessitates replacing of physical components or reinstalling an operating system or dataset.[61] This approach recognizes that the disabling of ICT systems or infrastructure can produce effects comparable to physical damage, even if no tangible destruction occurs.

Most States that have taken a position on this issue, however, adopt an even broader interpretation, according to which loss of functionality alone – without the need for physical

---

[56] Kubo Mačák and Laurent Gisel, 'The Legal Constraints of Cyber Operations in Armed Conflicts', in R Pillai Rajagopalan (ed), *Future Warfare and Technology: Issues and Strategies* (Wiley 2022) 147.

[57] Michael N Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) (*Tallinn Manual 2.0*) 415.

[58] Danish Ministry of Defence, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (Defence Command Denmark 2016) (Danish Military Manual) 677; Ministry of Foreign Affairs of Finland, *International law and cyberspace: Finland's national positions* (2020) (National position of Finland) 7; New Zealand Defence Force, *Manual of Armed Forces Law: Vol. 4* (2017), para 8.10.22 (New Zealand Military Manual); Norway, *Manual i krigens folkerett* (2013) (Norwegian Military Manual) para 9.54; Federal Department of Foreign Affairs of Switzerland, *Switzerland's position paper on the application of international law in cyberspace: Annex UN GGE 2019/2021* (FDFF 2021) 10; United States, *United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15)* 6; see also *ICRC position paper* (n 45) 7.

[59] See, eg, Jeppe Mejer Kjelgaards and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) 92 *Nordic Journal of International Law* 446, 455; Roy Schondorf, 'Israel's perspective on key legal and practical issues concerning the application of international law to cyber operations' (2021) 97 *International Law Studies* 395, 400 (National position of Israel); Peru, Response Submitted by Peru to the Questionnaire on the Application of International Law in OAS Member States in the Cyber Context (June 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1 (7 August 2020) Annex B, para 31.

[60] See, eg, National position of Israel (n 59) 400–401.

[61] *Tallinn Manual 2.0* (n 57) 417.

damage – suffices to classify a cyber operation as an attack.[62] For example, Austria has recently clarified that it considers operations that disable ICT systems or infrastructure to fall within the definition of attack under IHL.[63] On this view, the mere loss of usability of an ICT system, regardless of how it may be restored, would meet the threshold of damage qualifying a cyber operation as an attack.[64] This approach is arguably the most protective for potential victims of cyber operations and thus aligns with the object and purpose of the rules governing the conduct of hostilities.[65] As such, we consider it the most compelling interpretation that best reflects the realities of the digital age.

Given the disruptive effects that cyber operations can have on essential services, regardless of whether physical damage occurs, it is crucial to clarify where exactly the line between attacks and other cyber operations is drawn.[66] For instance, operations like cyber espionage generally fall outside the scope of the IHL concept of 'attack'.[67] However, such operations are not conducted in a legal vacuum. On the contrary, cyber operations that do not qualify as attacks remain subject to several IHL rules aimed at protecting civilians and civilian objects.

These include the obligation to exercise care to spare the civilian population and civilian objects during military operations.[68] Additional restrictions prohibit operations directed against specifically protected objects, such as medical facilities,[69] or operations designed to disable objects indispensable to the survival of the civilian population, such as water supply systems or agricultural infrastructure.[70] Thus, even when a cyber operation does not meet the definition of an attack, IHL continues to impose significant constraints on how such operations may be conducted.

IV. 2. The principle of distinction: Protecting civilians and civilian data

A core principle of IHL is the obligation to distinguish at all times between civilians and civilian objects on the one hand, and combatants and military objectives on the other.[71] Attacks may only be directed against combatants and military objectives, while civilians and civilian objects must be spared.

Therefore, just like anyone else, persons who use ICTs are protected from being attacked, unless they are combatants or civilians directly participating in hostilities. Given the victim-focus of this

---

[62] See the national positions of Austria, Costa Rica, France, Germany, Ireland, Italy, Japan, and New Zealand, as excerpted in 'Attack (international humanitarian law)' *Cyber Law Toolkit* (21 January 2025) <https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law)> accessed 31 January 2025; see also ICRC, *Challenges Report* (2024) (n 51) 49; *Council of Advisers' Report* (n 20) 38.

[63] National position of Austria (n 55) 17.

[64] See also *Tallinn Manual 2.0* (n 57) 418.

[65] Mačák and Gisel (n 56) 147; *ICRC position paper* (n 45) 7–8; Gisel, Rodenhäuser and Dörmann (n 12) 312–316.

[66] Mačák and Gisel (n 56) 147.

[67] *Tallinn Manual 2.0* (n 57) 415.

[68] The application of this rule to cyber operations has been affirmed by States including Austria, the Czech Republic, Costa Rica, Denmark, Finland, France, and Germany. See 'Principle of precautions' *Cyber Law Toolkit* (9 December 2024) <https://cyberlaw.ccdcoe.org/wiki/Principle_of_precautions> accessed 31 January 2025.

[69] See GC I, Art 19; GC IV, Art 18; AP I, Art 12; AP II, Art 11(1); *ICRC CIHL Study* (n 32) Rule 28. See also *Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector* (21 May 2020) para 5.

[70] AP I, Art 54; AP II, Art 14; *ICRC CIHL Study* (n 32) Rule 54. See also UN Security Council, Res 2573 (2021) UN Doc S/RES/2573 (27 April 2021).

[71] *ICRC CIHL Study* (n 32) Rules 1 and 7.

chapter, we leave the question of combatancy aside[72] and focus on the notion of direct participation in hostilities in the cyber context – a topic on which several States have expressed views.[73] The United Kingdom, for instance, has stated that individuals carrying out cyber operations that qualify as attacks are directly participating in hostilities and are therefore targetable.[74] France and Germany have also discussed the possibility that engagement in cyber operations may amount to direct participation in hostilities, while relying on the ICRC's 2009 guidance[75] for the relevant criteria.[76]

Persons fulfilling the criteria of directly participating in hostilities might include individual hackers or hacker groups launching cyber operations to support their side's war efforts. For example, the act of cyber interference with the computer network of a railway company during an armed conflict to block the deployment of trains carrying military equipment belonging to the enemy may qualify as direct participation in hostilities.[77] This growing phenomenon inspired the ICRC to formulate eight core rules for hackers involved in armed conflicts, alongside four obligations for States to restrain civilian hackers and thereby mitigate the civilianization of the digital battlefield.[78]

Two challenges emerge from the difficulty of attributing cyber operations to specific individuals. First, as noted by France, targeting the person conducting an attack through cyber means will often be impractical in real-time situations.[79] Second, cyberspace creates unique difficulties in determining an individual's status or activity, making it essential to emphasize that, in case of doubt, a person must be presumed to be a civilian and, therefore, protected from attack.[80]

In addition to persons, the principle of distinction also governs cyber activities affecting objects. All objects are protected from attack – including using cyber means – unless they qualify as military objectives, as defined in Article 52(2) of Additional Protocol I.[81] This raises a critical question about

---

[72] For a recent analysis, see Mačák (n 31) 419–421.

[73] For an overview, see 'Direct participation in hostilities' *Cyber Law Toolkit* (21 September 2021) <https://cyberlaw.ccdcoe.org/wiki/Direct_participation_in_hostilities> accessed 31 January 2025.

[74] United Kingdom, Foreign, Commonwealth & Development Office, *Application of international law to states' conduct in cyberspace: UK statement* (3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement> accessed 31 January 2025.

[75] ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) (*ICRC DPH Guidance*).

[76] National position of France (n 49) 15; National position of Germany (n 55) 8.

[77] For a recent example, see Ryan Gallagher, '"Cyber Partisans" Say They Hacked Belarus Rail to Disrupt Russian Troops', *Bloomberg* (24 January 2022) <https://www.bloomberg.com/news/articles/2022-01-24/hackers-say-they-breached-belarusian-rail-to-stop-russian-troops> accessed 31 January 2025.

[78] ICRC, 'Eight rules for "civilian hackers" during war, and four obligations for states to restrain them' (2 August 2024) <https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them> accessed 31 January 2025.

[79] National position of France (n 49) 15.

[80] AP I, Art 50(1). See also *ICRC DPH Guidance* (n 75) 75–76 (affirming the presumption of protection in cases of doubt as to whether a specific civilian conduct qualifies as direct participation in hostilities). Similarly, see, eg, New Zealand Military Manual (n 58) 6-15, para 6.5.11. But see *Tallinn Manual 2.0* (n 57) commentary to rule 97, para 13, noting that the 'International Group of Experts was divided over the issue of whether a presumption against direct participation applies'.

[81] See AP I, Art 52(2): 'In 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.'

whether civilian data – such as social security records, taxation data, or electoral datasets – qualifies as a civilian object and thus benefits from IHL protections.

One view argues that data, being immaterial, invisible and intangible, cannot be considered an object under IHL.[82] States that subscribe to this view include Denmark,[83] Chile,[84] and Israel.[85] This interpretation would, however, leave cyber operations targeting civilian data outside the scope of those conduct of hostilities rules that pertain solely to civilian objects, creating a significant protection gap.[86]

An alternative perspective – which we agree with – holds that the term 'object' should be interpreted broadly to align with IHL's humanitarian purpose.[87] This is because cyber operations interfering with civilian data can disrupt government services, harm private businesses, and affect individuals, underscoring the need to apply IHL protections to such data.[88] Accordingly, a growing number of States – including Austria,[89] Costa Rica,[90] Finland,[91] Germany,[92] Norway,[93] and Romania[94] – take the view that the protection of civilian objects extends to civilian data.

IV. 3. The principle of proportionality: Limiting harm in interconnected systems

The principle of proportionality protects civilians and civilian objects from incidental harm that would be excessive in relation to the concrete and direct military advantage anticipated from an attack targeting a military objective.[95] This *ex ante* assessment of proportionality requires a careful balancing of expected incidental civilian harm against the military advantage of the attack. Importantly, this assessment must account for both direct and indirect harm to civilians and civilian objects.

While some contention remains around the type of damage to civilian objects that must be included in this balancing act, most experts agree that it is not limited to physical damage alone.[96] In particular, non-tangible harm to civilians, such as psychological and social harm that exceeds

---

[82] *Tallinn Manual 2.0* (n 57) commentary to rule 100, para 5.

[83] Danish Military Manual (n 58) 292.

[84] Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc CJI/doc. 615/20 rev.1 (7 August 2020) para 36.

[85] National position of Israel (n 59), 401.

[86] Mačák and Gisel (n 56) 148.

[87] See, eg, Robert McLaughlin, 'Data as a Military Objective', *Australian Institute of International Affairs* (20 September 2018) <https://www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/> accessed 31 January 2025.

[88] See further Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 *Israel Law Review* 55.

[89] National position of Austria (n 55) 18.

[90] National position of Costa Rica (n 48) para 50.

[91] National position of Finland (n 58) 7.

[92] National position of Germany (n 55) 8.

[93] Norwegian Military Manual (n 58) para 9.58.

[94] UN, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, UNODA, UN Doc A/76/136 (August 2021) 78.

[95] AP I, Arts 51(5)(b) and 57(2)(a)(iii)(b); *ICRC CIHL Study* (n 32) Rule 14.

[96] *Tallinn Manual 2.0* (n 57), commentary to rule 92, paras 10–12. *ICRC position paper* (n 45) 7–8.

mere 'inconvenience, irritation, stress, or fear' must also be considered.[97] To the extent that loss of functionality is recognized as a form of damage (see section IV.2 above), it logically follows that the disabling of civilian ICT systems or infrastructure, even in the absence of physical destruction, must also be included as incidental civilian harm.[98]

A commander conducting a proportionality assessment in the cyber context must also consider the unique characteristics of cyberspace, particularly the interconnected nature of ICTs.[99] Cyber tools such as malware can spread quickly and widely, potentially causing cascading effects or a ripple of indirect damage to civilian systems and infrastructure. These effects may include disruptions to critical services such as healthcare, transportation, or energy, which could severely impact civilian populations.

Another significant consideration is the potential for incidental civilian harm to occur in the territory of a State that is not party to the armed conflict.[100] Such harm, even if geographically removed from the area of hostilities, is not exempt from the proportionality analysis.[101] All reverberating effects, provided they are reasonably foreseeable at the time of the attack, must be considered when determining whether the incidental harm to civilians is excessive.[102]

In the context of cyber operations, where the interconnectedness of ICT systems amplifies the potential for cascading harm, the principle of proportionality serves as a vital safeguard to limit the harm incurred by civilians and civilian objects. While the effects may be harder to foresee than with kinetic weapons, this makes it all the more crucial to take all feasible steps to assess potential harm – a key aspect of precautions under IHL, to which we now turn.

IV. 4. The principle of precautions: Mitigating cyber-enabled harm

In addition to prohibitive rules, the conduct of hostilities regime under IHL contains a host of positive obligations that require parties to a conflict to take certain protective steps. These obligations to take precautions supplement the principles of distinction and proportionality. In particular, IHL imposes obligations on those planning, deciding on, or carrying out attacks ('active precautions'), and it also requires parties to armed conflicts to protect civilians and civilian objects under their control from the effects of attacks ('passive precautions').

With respect to **active precautions**, parties to armed conflicts must take all feasible steps to avoid, and in any event minimize, incidental loss of civilian life, injury to civilians and damage to

---

[97] *Tallinn Manual 2.0* (n 57), commentary to rule 113, para 5.

[98] See also National position of Austria (n 55) 19 ('When assessing incidental civilian harm, possible non-kinetic effects of an attack, such as the temporary deprivation of functionality of an ICT system, and possible indirect effects, need to be considered.'); National position of Costa Rica (n 55) para 47 ('In Costa Rica's view, the incidental harm to be taken into consideration includes any incidental loss of functionality of civilian computers, systems or networks.').

[99] ICRC, *Cyber Operations During Armed Conflict: The principle of proportionality* (March 2023); see also Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94(886) International Review of the Red Cross 533, 571–573.

[100] Jonathan Horowitz and Florentina Pircher, 'Scenario 28: Extraterritorial incidental civilian cyber harm' *Cyber Law Toolkit* (14 May 2024) <https://cyberlaw.ccdcoe.org/wiki/Scenario_28:_Extraterritorial_incidental_civilian_cyber_harm> accessed 31 January 2025.

[101] Ibid.

[102] For State views in support of this view, see fn 58 above.

civilian objects when launching an attack.[103] For cyber operations that qualify as attacks, precautionary measures must also address the risks of harm specific to cyberspace. This includes assessing the interconnectedness of military and civilian networks, identifying potential secondary effects on essential civilian infrastructure, and evaluating whether malware or other tools could unintentionally spread beyond the intended target.[104]

Passive precautions, which have already been discussed in part as obligations that States must implement in peacetime (see section III.2 above), also require defending forces to protect the civilian population and civilian objects under their control during armed conflicts.[105] In the cyber context, this obligation translates into specific measures to mitigate harm from potential cyber intrusions. For example, enhancing cybersecurity protocols for critical civilian infrastructure – such as power grids, water supplies, and healthcare systems – can help defend against the effects of cyber operations. Similarly, implementing redundancy systems to ensure the continuity of essential services, even if primary networks are disrupted, serves as an important safeguard.[106]

These precautionary measures are particularly vital in cyberspace, where the risks of cascading and unpredictable effects are amplified by the interconnected nature of ICT systems. Both active and passive precautions represent indispensable components of the broader effort to uphold IHL in the digital age, ensuring that civilian populations and infrastructure are afforded the maximum protection possible in times of conflict.

V. Ensuring accountability for cyber-enabled violations of IHL

V. 1. Pathways to accountability

Accepting that IHL applies to cyber operations inevitably means that cyber operations can violate IHL. States, armed groups, and individuals may violate IHL through cyber means, and the consequences of such violations remain the same under the applicable rules of international law. This includes State responsibility for acts that are attributable to a State,[107] the obligation to make full reparation for loss or injuries caused,[108] and the duty to investigate and prosecute war crimes within a State's jurisdiction.[109]

Individuals may also incur criminal responsibility for serious violations of IHL through cyber means.[110] The Office of the Prosecutor (OTP) of the International Criminal Court (ICC) has

[103] AP I, Art 57; *ICRC CIHL Study* (n 32) Rule 15.

[104] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2015) 43; see also ICRC, *Avoiding Civilian Harm* (n 16) 26–27.

[105] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987) para 2239.

[106] ICRC, *Avoiding Civilian Harm* (n 16) 27–28.

[107] *ICRC CIHL Study* (n 32) Rule 149

[108] Ibid, Rule 150

[109] Ibid, Rule 158.

[110] *Tallinn Manual 2.0* (n 57) Rule 84; *Council of Advisers' Report* (n 20) 27; Kai Ambos, 'International Criminal Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on Cyberspace and International Law* (2nd edn, Edward Elgar 2021) 156.

recognized the potential for cyber-enabled international crimes, and it is expected to publish a detailed policy on this issue in 2025.[111]

This development is significant for several reasons. First, the OTP's efforts to collect and analyse evidence related to cyber operations will contribute to building expertise and capacity to address cyber-enabled IHL violations.[112] For example, the ICC could investigate cases where cyber operations targeted protected civilian infrastructure, such as disabling hospital systems during armed conflict.[113] Second, it may lead the OTP to focus on cases where cyber operations are used to facilitate or amplify kinetic strikes or other grave crimes already under investigation.[114] For instance, co-ordinated cyber and kinetic attacks documented in the ongoing armed conflict between Russia and Ukraine demonstrate how cyber operations can amplify the impact of conventional warfare and could fall within the ICC's purview.[115] Third, the OTP may also investigate and prosecute cyber operations aimed at obstructing the administration of justice at the ICC itself,[116] an increasingly plausible threat.[117]

V. 2. Overcoming challenges in prosecuting cyber-enabled crimes

Despite these developments, prosecuting cyber-enabled war crimes and other international crimes presents unique challenges. Chief among these is attributing cyber operations to their authors. The anonymity afforded by cyberspace makes it significantly easier for individuals to remain untraceable or to act through proxies, as compared to kinetic crimes. Even when technical methods successfully trace the origin of a cyber operation to a specific machine, identifying the human actor responsible and meeting the stringent standard of proof required for criminal liability remains a formidable challenge.[118] The proliferation of ICT capabilities among non-State actors further exacerbates difficulties in attribution, often making it hard to identify those responsible for ordering or carrying

---

[111] ICC, *The Law in Action For All: Office of the Prosecutor Annual Report 2024* (2024) 106.

[112] For instance, the OTP has stated it would be supporting States' capacities in collecting and reviewing evidence on cyber operations. Karim A A Khan KC, 'Technology Will not Exceed our Humanity' *Digital Front Lines* (20 August 2023) <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/> accessed 31 January 2025.

[113] See, eg, Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?', *Just Security* (27 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 31 January 2025.

[114] Milena Sterio and Jennifer Trahan, 'Cyber Operations as Crimes at the International Criminal Court' *Articles of War* (4 October 2023) <https://lieber.westpoint.edu/cyber-operations-crimes-icc/> accessed 31 January 2025.

[115] See Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (22 June 2022) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK> accessed 31 January 2025.

[116] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 (Rome Statute), Art 70(1); Khan (n 112).

[117] See ICC, 'Measures taken following the unprecedented cyber-attack on the ICC' (20 October 2023) <https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc>. Media reports have suggested that some of the interference may have been attributable to Israel's intelligence services: see Harry Davies et al, 'Spying, hacking and intimidation: Israel's nine-year 'war' on the ICC exposed', *The Guardian* (28 May 2024) <https://www.theguardian.com/world/article/2024/may/28/spying-hacking-intimidation-israel-war-icc-exposed> accessed 31 January 2025.

[118] Rome Statute, Art 66(3), requiring proof beyond reasonable doubt. See further, eg, Kubo Mačák and Maxime Nijs, 'Hackers in the Hague? The Prospects of Prosecuting International Cyber Crimes Before the ICC' *Lawfare* (18 October 2023) <https://www.lawfaremedia.org/article/hackers-in-the-hague-the-prospects-of-prosecuting-international-cyber-crimes-before-the-international-criminal-court> accessed 31 January 2025.

out cyber operations.[119] These challenges hinder accountability efforts and reduce the deterrent effect of criminalization.[120]

Another significant challenge lies in quantifying the harm caused by cyber operations. As discussed in section II, cyber harm often takes diverse forms – physical, psychological, social, and economic – and the complexity of cyberspace can lead to unpredictable consequences. For instance, a cyber operation against a war-torn country's power grid that cuts electricity to hospitals, water treatment plants, and sanitation systems could result in widespread harm to civilians, potentially meeting the ICC's gravity threshold.[121] While these factors may complicate the prosecution of cyber-enabled IHL violations, they also invite us to rethink conventional understandings of the harm caused by kinetic warfare, recognizing that the impact of cyber operations can be equally, if not more, far-reaching.[122]

Although cyber-enabled crimes are sometimes still referred to as the 'crimes of the future',[123] they have already become part of present-day reality. Addressing the challenges of prosecuting these crimes requires close co-operation among States, experts, and private corporations. For instance, Microsoft has partnered with the ICC to help overcome current obstacles to accountability for cyber-enabled crimes, offering a promising example of how public-private collaboration can advance justice in the digital age.[124]

Ultimately, ensuring accountability for cyber-enabled IHL violations is essential for upholding the rights of victims and preventing future harm. By addressing the unique challenges of prosecuting the criminalized IHL obligations, the international community can better deter future violations and protect civilians from the unique risks posed by cyber operations in armed conflict.

VI. Conclusion

The rapid development of ICTs has brought unparalleled opportunities and significant risks, which are particularly pronounced in the context of armed conflict. Cyber operations have become a critical component of modern warfare, presenting unique challenges for the protection of civilians

---

[119] *Council of Advisers' Report* (n 20) 3; Johan Sigholm, 'Non-State Actors in Cyberspace Operations' (2013) 4 *Journal of Military Studies* 1, 9–23.

[120] See Gary D Brown, 'Some Nondestructive State Cyber Operations Probably Constitute the Crime of Aggression under the Rome Statute, but Attribution Difficulties and State Practice Make Effective Deterrence Unlikely', *ICC Forum* (7 March 2022), <https://iccforum.com/cyberwar#Brown> accessed 31 January 2025.

[121] See Rome Statute, Article 17(1)(d), requiring that a case must be of 'sufficient gravity to justify … action by the Court'. See further Jennifer Trahan, 'The Criminalization of Cyber-operations Under the Rome Statute' (2021) 19(5) *JICJ* 1133, 1138–1146.

[122] See, further, the discussions on reverberating effects of explosive weapons in urban areas and on psychological harm caused by warfare. Mark Zeitoun and Michael Talhami, 'The impact of explosive weapons on urban services: Direct and reverberating effects across space and time' (2016) 98(1) *International Review of the Red Cross* 53; ICRC, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities Under International Humanitarian Law* (22–23 June 2016) 34–36; Eliav Lieblich, 'Beyond Life and Limb: Exploring Incidental Mental Harm Under International Humanitarian Law', in Derek Jinks, Jackson N Maogoto and Solon Solomon (eds), *Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies: International and Domestic Aspects* (Asser Press 2014) 201.

[123] See Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system (22 January 2024) <https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through> accessed 31 January 2025.

[124] 'Tech sector to help international justice fight cyber-enabled crimes' *Intelligence Online* (18 March 2024) < https://www.intelligenceonline.com/surveillance--interception/2024/03/18/tech-sector-to-help-international-justice-fight-cyber-enabled-crimes,110192323-art> accessed 31 January 2025.

and civilian infrastructure. This chapter has explored the harm that cyber operations can inflict during armed conflicts, the legal protections offered under international law, and the accountability mechanisms necessary to address violations.

The harms posed by cyber operations during armed conflicts are diverse and far-reaching, affecting civilians in multiple ways. This chapter has proposed five categories, which include (1) direct harm to civilians, civilian systems and services; (2) risks stemming from the civilianization of the digital battlefield; (3) psychological, social, and economic impacts; (4) systemic and interconnected risks; and (5) risks of conflict escalation. These categories highlight the complex ways in which cyber operations can endanger civilian populations and amplify the humanitarian consequences of armed conflicts, underscoring the need for comprehensive legal and policy responses.

IHL offers a robust framework for safeguarding civilians, even in the face of novel challenges posed by new technologies such as cyber capabilities. Its core principles – distinction, proportionality, and precautions – are technology-neutral. They can and must be applied to cyber operations, thereby confirming IHL's adaptability and enduring relevance. However, the effective implementation of these principles requires States and other parties to armed conflicts to clarify their legal positions, enhance their technical capacities, and adopt measures to mitigate risks before and during armed conflicts.

Accountability for cyber-enabled violations of IHL is equally essential for upholding the rule of law and deterring future violations. While the application of international criminal law to cyber operations is still nascent, the ICC OTP's recognition of cyber-enabled crimes marks a significant step forward. Efforts by States, international organizations, and private actors to strengthen investigative and prosecutorial capacities will be critical to overcoming the challenges of attribution, quantification of harm, and ensuring justice for victims.

Ultimately, the protection of civilians and civilian infrastructure in the digital age requires not only the rigorous application of existing legal frameworks but also enhanced co-operation across sectors and borders. As cyber operations continue to evolve, so too must the international community's commitment to addressing their humanitarian impact, ensuring that the benefits of technological progress do not come at the expense of fundamental legal safeguards in times of war.