HUMANITARIAN
LAW & POLICY

Towards common understandings: the application of established IHL principles to cyber operations

March 7, 2023, Analysis / Avoiding civilian harm during military cyber operations / Human Costs of Cyber / Law and Conflict / New Technologies

9 mins read


Kubo Mačák
Legal Adviser, ICRC


Tilman Rodenhäuser
Thematic Legal Adviser, ICRC

Cyber operations have become a reality of today's armed conflicts, and their use is likely to continue to grow in the future. In light of this trend, the ICRC has long maintained that international humanitarian law (IHL) governs – and limits – any use of cyber operations during armed conflicts. But what does that really mean in practice?

In this post, ICRC legal advisers Kubo Mačák and Tilman Rodenhäuser provide concise explanations of when and how IHL – and especially its principles of humanity, necessity, distinction, and proportionality – apply to the use of information and communications technologies (ICTs) by States. With this post, they launch the ICRC's new series of short papers on cyber operations during armed conflict.

A recent *study* estimates that over 60 States have formed active-duty cyber forces within their military structures. Parties to armed conflicts – and a range of actors with non-governmental or unclear affiliations – have used military cyber capabilities in the context of contemporary armed conflicts, at times as

stand-alone operations, at times in co-ordination with kinetic operations. The ongoing international armed conflict between Russia and Ukraine is only the most recent illustration.

That these developments may bear significant human cost is hardly news in 2023. As early as 2001, Knut Dörmann, ICRC legal adviser at the time, *warned* that cyber operations launched against industries, infrastructures, or telecommunications could bring about devastating consequences if certain system malfunctions were caused. Today, this assessment is echoed in consensus statements by States at the highest levels: for instance, a UN-mandated open-ended working group *affirmed* in 2021 that cyber operations may seriously affect civilian infrastructure and thus result in 'devastating humanitarian consequences' (para. 18).

Digital threats to civilian populations urgently require inclusive discussions – and clarifications – of complex legal questions. What limits do existing rules of IHL impose on cyber operations that risk disrupting essential civilian services and infrastructure or manipulate and delete data? Who is responsible for the conduct of non-State actors in the ICT environment, what obligations do these actors have, and what consequences do they face if they take part in hostilities?

Yet, the regulatory response at the international level has been rather cautious. Although multilateral discussions related to 'information security' started already in 1998 when the Russian Federation introduced a first *resolution* on the subject, it took until 2013 for a *UN Group of Governmental Experts (GGE)* to achieve a *consensus* on the baseline issue that international law is applicable in cyberspace (para. 19).

The issue of cyber operations during armed conflict has also long been on the agenda of multilateral discussions. In 2015, a subsequent GGE *noted* 'the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction' (para. 28(d)). Six years later, the final GGE *expressly linked* those principles to the body of law to which they belong, that is, international humanitarian law (para. 71(f)). In the same report, the GGE recognized the need for further study on 'how and when' these principles apply to the use of ICTs by States (ibid.).

Today, the ICRC issues four short papers intended to support further discussions precisely on those 'how' and 'when' questions. They will be formally presented in New York during the international law segment of the ongoing UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, the *mandate* of which includes the development of common understandings on the application of international law in the ICT environment. In addition, we hope that the content of these papers will be of interest to the broader community of international law practitioners and scholars working in the area.

Here, we briefly explain when and how IHL and its key principles apply in the ICT environment. On each issue, we include a short explanation of what it means (represented in bold at the top of the paper in question), a brief overview of the paper's content, and a link to its full text, where you can find out more.

Paper #1: When does international humanitarian law apply to the use of information and communications technologies?

International humanitarian law applies to the use of information and communications technologies in situations of armed conflict.

One part of the answer to the question of 'when' IHL applies is as simple as it is important: as *noted* by the GGE, IHL applies only in situations of armed conflict (putting aside certain exceptions, on which see e.g. *this article*, note 2). It should be remembered that determining when IHL applies is legally distinct from the question of which conduct amounts to a prohibited 'threat or use of force' or an 'armed attack' under the UN Charter. Situations in which IHL applies are either armed conflicts between States ('international armed conflicts') or armed conflicts between States and non-State armed groups, or between such groups ('non-international armed conflicts'). The paper analyses which situations involving the use of cyber capabilities may qualify as one of those types of armed conflict. While certain aspects of the applicable law remain unsettled, there is no question that IHL applies when a cyber operation is carried out in conjunction with or in support of classic 'physical' or 'kinetic' military operations in the context of an existing armed conflict.

Read the full paper here.

Paper #2: The principles of humanity and necessity under IHL

The fundamental principles of humanity and military necessity underlie and inform the entire normative framework of international humanitarian law. All rules of IHL reflect a careful balance between these two principles, which in turn inform the interpretation of these rules. The two principles also impose limits beyond specific rules, including in the information and communications technology environment.

Since the *1868 St Petersburg Declaration*, it has been understood that through the development of IHL, States continuously recalibrate when, and to what extent, 'the necessities of war ought to yield to the requirements of humanity'. Thus, the first two of the four 'established legal principles' noted by the GGE in 2015 are dealt with in a single paper. The paper explores how the two closely related principles of humanity and military necessity affect the application and interpretation of IHL in the cyber context. It shows that they are particularly important in cases where the interpretation of existing rules – for instance, the *rule* defining 'attack' under IHL – to cyber operations is unsettled.

Read the full paper here.

Paper #3: The principle of distinction under IHL

In the use of information and communications technologies, the principle of distinction requires that parties to an armed conflict at all times distinguish between civilians and combatants and between civilian objects and military objectives. Cyber attacks may only be directed against combatants or military objectives. Cyber attacks must not be directed against civilians or civilian objects. Indiscriminate cyber attacks are prohibited.

The International Court of Justice has *described* the principle of distinction as a 'cardinal' and 'intransgressible' principle that forms part of the 'fabric' of IHL (paras 78-79). The principle requires parties to armed conflicts to refrain from launching cyber operations that qualify as attacks against civilian objects and infrastructure. The principle of distinction also prohibits indiscriminate attacks, including when using cyber means or methods of warfare. The paper further discusses how the principle of distinction limits cyber operations other than attacks. Finally, it considers how the respect for this principle can be ensured in the cyber context, including through responsible development of cyber tools and careful target verification. Its recommendations – like those in the following paper – are based on the ICRC's close engagement with technical experts, which we have also covered on *this blog*.

Read the full paper here.

Paper #4: The principle of proportionality under IHL

In the use of information and communications technologies, the principle of proportionality prohibits parties to armed conflicts from launching a cyber attack against a military objective which may be expected to cause incidental civilian harm that would be excessive in relation to the concrete and direct military advantage anticipated.

The principle of proportionality under IHL is crucial for protecting civilians and civilian infrastructure in times of armed conflict, and particularly so in the interconnected ICT environment. It limits the extent of incidental civilian harm that is permissible when parties to armed conflicts attack military objectives, including through cyber means and methods of warfare. The paper explains that the assessment of incidental harm must include both direct and indirect effects of cyber operations. It recommends that States that foresee resorting to cyber operations during armed conflicts should adapt the existing procedures for assessing compliance with the principle of proportionality (sometimes also called 'collateral damage estimation methodologies') to account for the specific challenges posed by the ICT environment.

Read the full paper here.

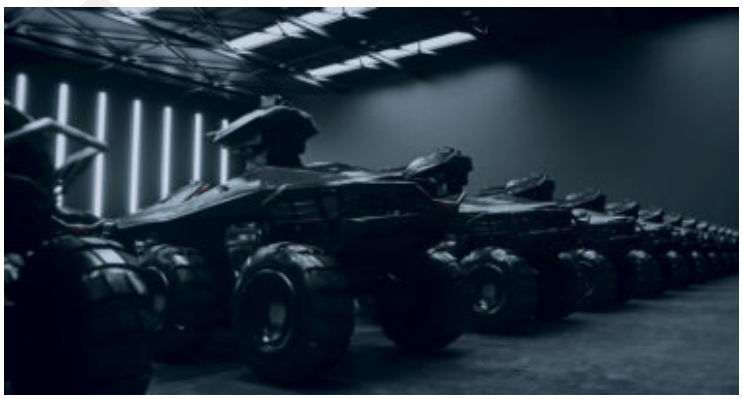
With these four papers, the ICRC aims to inform the existing debates on the application of IHL to cyber operations during armed conflict. They are not intended nor phrased as final answers to the questions and principles they address, but rather as a means to build capacity and to advance conversation. We believe that through such discussions, we can get closer to common understandings on the application and interpretation of IHL in the cyber context, thereby safeguarding civilians, civilian data, and civilian infrastructure from the harmful effects of cyber operations during armed conflict.

See also

- Pete Renals, *Future developments in military cyber operations and their impact on the risk of civilian harm*, June 24, 2021
- Ellie Shami, *Assessing the risks of civilian harm from military cyber operations during armed conflicts*, June 22, 2021
- Noëlle van der Waag-Cowling, *Stepping into the breach: military responses to global cyber insecurity*, June 17, 2021
- Kubo Mačák & Ewan Lawson, *Avoiding civilian harm during military cyber operations: six key takeaways*, June 15, 2021

Tags: armed conflict, cyber, cyber attacks, cyber operations, cyber warfare, digital technology, IHL, international humanitarian law, international law, LOAC, military cyber operations, protection of civilian population, Russia, Ukraine, United Nations

You may also be interested in:

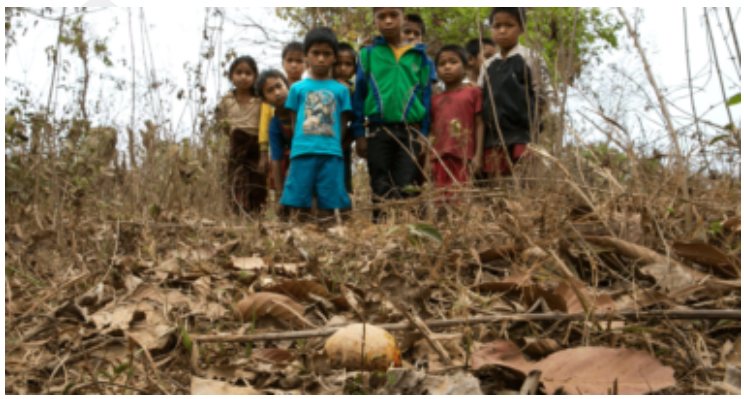


Three lessons on the regulation of autonomous weapons systems to ensure accountability for violations of IHL

11 mins read

Analysis / Avoiding civilian harm during military cyber operations / Human Costs of Cyber / Law and Conflict / New Technologies

Vincent Boulanin & Marta Bo



Preventing and eradicating the deadly legacy of explosive remnants of war

13 mins read

Analysis / Avoiding civilian harm during military cyber operations / Human Costs of Cyber / Law and Conflict / New Technologies Eirini Giorgou

The deadly legacy of armed conflict continues to claim lives long after the fighting is …

States have agreed on the principle that machines cannot be held accountable for violations of …