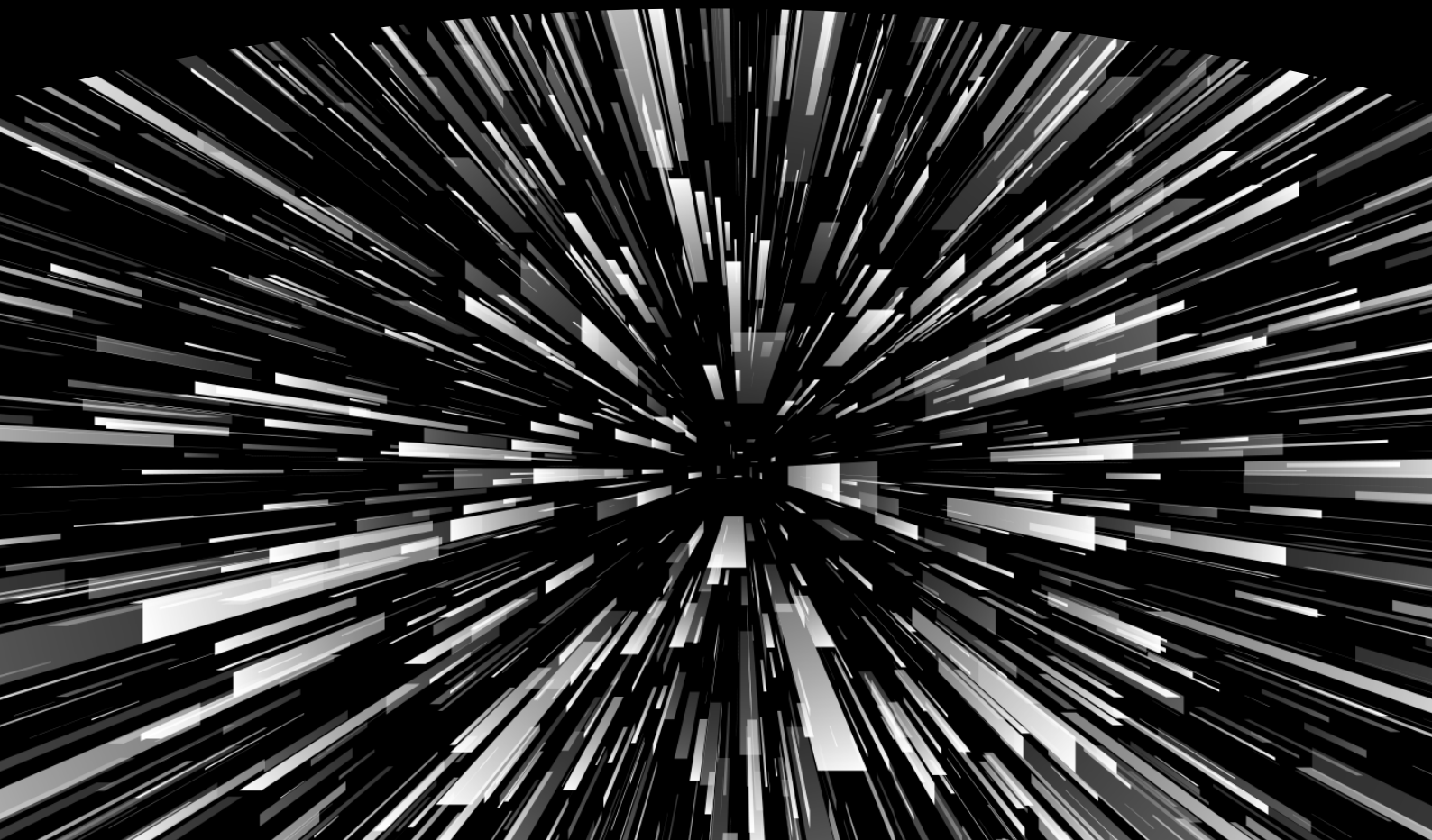
UNIDIR

REPORT

International Humanitarian Law and Cyber Operations: (Consequences of) Divergent National Interpretations of “Attack” and “Data”

GIACOMO BIGGIO AND ANDRAZ KASTELIC



Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. Work on international cybersecurity by UNIDIR's Security and Technology Programme is funded by the Governments of Germany, Italy, the Netherlands, Switzerland and by Microsoft.

The authors extend their gratitude to Dominique Steinbrecher, Samuele Dominioni, Giacomo Persi Paoli (UNIDIR), Marco Roscini (University of Westminster) and Tilman Rodenhäuser (International Committee of the Red Cross) for providing their thoughts on various drafts of this paper. The analysis and views presented in this paper are, however, only those of the authors and may not be shared by reviewers.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Cover photography: 3d_kot/Shutterstock. Design and layout by Kathleen Morf.
www.unidir.org – © UNIDIR 2026

Authors

Giacomo Biggio

Lecturer in law and co-director of the Human Rights Implementation Centre at the University of Bristol Law School.

Andraz Kastelic

Senior researcher and coordinator of the International Cyber Resilience Workstream of the Security and Technology Programme of UNIDIR.

Abbreviations

GGE	Group of Governmental Expert
ICRC	International Committee of the Red Cross
ICT	Information and communications technology
IHL	International humanitarian law
OEWG	Open-Ended Working Group
SCADA	Supervisory control and data-acquisition

Contents

Executive summary

The application of international humanitarian law (IHL) to cyber operations during armed conflict is complex. Even after more than a decade of multilateral discussions in such forums as the United Nations groups of governmental experts and open-ended working groups, a common understanding of how IHL applies in cyberspace – the information and communications technology (ICT) domain – remains elusive. Notably, there are divergent interpretations of "attack" and of whether "digital data" is an object under IHL. This deficiency of clarity, particularly concerning what constitutes permissible or impermissible cyber behaviour in armed conflict, could inhibit legal protections of civilians and civilian objects.

In an effort to facilitate future multilateral discussions on how international law, and in particular IHL, applies to cyber operations, this paper highlights two main interpretive approaches found in scholarship and, most importantly, national positions on international law in cyberspace:

- A restrictive interpretation, which limits the notion of "attack" under IHL to cyber operations that cause physical harm and generally excludes digital data as an object
- An expansive interpretation, which includes operations that result in a "loss of functionality" within the notion of attack and considers essential civilian data as a legally protected object

Analysis of national positions reveals a divergence, with some States aligning with a restrictive interpretation, others adopting an expansive one and some calling for further study.

Hypothetical scenarios demonstrate how these differing interpretations can lead to significantly different legal outcomes regarding obligations in the conduct of hostilities. This applies in particular to the assessment of proportionality and precaution, especially when a cyber operation does not cause physical damage but results in data deletion or loss of functionality.

To enhance legal clarity and continue building common understanding of the application of international law in cyberspace, States should continue to actively engage in multilateral discussions; articulate individual national positions on the application of IHL to cyber operations; and share legal analyses of observed, practical ICT incidents in armed conflicts. Relevant multilateral processes have encouraged the publication of national positions on the interpretation of IHL to foster transparency. This recommendation is worth reiterating since these views can be integrated into domestic governance frameworks such as military manuals and cybersecurity strategies. Ultimately, the paper argues that the incremental convergence of common understanding, while unlikely to ever achieve absolute uniformity, is crucial for establishing clearer international limits on the use of ICTs in armed conflict.

1. Introduction and context

Information and communications technologies (ICTs) have profoundly transformed modern society in the past decades. Their integration into day-to-day lives have brought invaluable positive effects as well as the potential for negative impacts.[1] As well as civilian uses, ICTs have military applications.[2] More specifically, not only are "a number of States… developing ICT capabilities for military purposes",[3] these technologies are also actively being used in ongoing armed conflicts around the world.[4] In such contexts, ICTs can not only be detrimental to international security and stability but can also potentially be used to harm civilian populations.

However, the ICT domain is by no means a lawless domain; indeed, States have agreed that their use of ICTs, including in the context of armed conflicts, is subject to the limitations of existing international law.[5] Specifically, in 2013 the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security agreed that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[6] This was subsequently confirmed by the United Nations General Assembly.[7] Moreover, in 2021 the General Assembly welcomed the final report of the GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which noted the need to explore further how the rules of international humanitarian law (IHL) are interpreted and applied in the ICT domain, while recognizing that IHL only applies in situations of armed conflict.[8]

IHL has received ample attention in the relevant multilateral negotiations on international law in cyberspace that have sought a common understanding of international law in cyberspace. However, the years of dedicated discussions have not yielded legal clarity on how IHL applies to cyberspace; most recently, for instance, the annual progress reports of the Open-ended Working Group (OEWG) on Security of and in the Use of ICTs 2021–2025 resorted to restatements of the relevant agreement of the 2021 GGE, including the need to study the topic further. The OEWG's final report went no further than acknowledging the increasing number of States that had expressed an opinion on how IHL applies to cyberspace.[9]

---

1 General Assembly, Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816, 18 March 2021, Annex I, paragraph 15.
2 General Assembly, resolution 53/70, 4 December 1998.
3 General Assembly, A/75/816, Annex I, paragraph 16.
4 34th Conference of the Red Cross and Red Crescent, resolution 34IC/24/R2, October 2024.
5 General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013; General Assembly, resolution 70/237, 30 December 2015.
6 General Assembly, A/68/98, paragraph 19.
7 See e.g. General Assembly, resolution 75/240, 31 December 2020, 3.
8 General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, paragraph 71(f).
9 General Assembly, Final Report of t he Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/80/257, 24 July 2025.

In addition to seeking common understanding on this issue through the multilateral deliberations under the auspices of the United Nations, States have also participated in "continued voluntary sharing of national views on international law which may include national statements and State practice on how international law applies in the use of ICTs by States".[10] To date, a limited number of States have taken a national position on interpretation of key IHL concepts in the digital domain: by the end of 2025, 36 States had published their national positions (along with regional positions by the African Union and the European Union); 32 of these feature interpretations of IHL in the context of cyber operations.[11] As demonstrated in the theoretical and practical contexts below, these national positions exhibit a degree of divergence.

This lack of common understanding could undermine compliance with IHL, erode accountability for transgressions, and ultimately inhibit the legal protections of civilians and civilian objects.

To facilitate the future multilateral discussion on how international law, and particularly IHL, applies to the ICT domain, this report outlines the spectrum of interpretations (as a form of evidence of *opinio juris* and an indication of State practice) of IHL in the context of cyber operations in an armed conflict. In doing so, it pays particular attention to the interpretations of the rules governing the conduct of hostilities: the principles of distinction, proportionality and precaution.

More specifically, this paper addresses two of the most challenging issues by exploring the meaning accorded to the **notion of "attack"** and **whether digital data can be considered as an object** for the purposes of IHL. The interpretations of these two concepts determine the scope and application of legal protections in an armed conflict – and these legal protections play a vital role in shielding civilians and civilian infrastructure from the effects of cyber operations during armed conflicts. Indeed, in line with the consensus outcomes of the relevant multilateral negotiations, States have recently noted the increased relevance of data protection and data security.[12]

Accordingly, Section 2 of the report introduces the notion of IHL and its main principles. Section 3 outlines interpretations of "attack" and Section 4 outlines interpretations of "object" as advanced by the scholarship and by States in their national positions, broadly distinguishing between restrictive and expansive interpretations and identifying areas of convergence and divergence among the interpretations. Section 5, based on a fictional scenario of a cyber operation in the context of an armed conflict, provides a practical analysis of different interpretations and identifies some of the outstanding challenges associated with the IHL notions of attack and object in the digital domain. Based on this, the final section, Section 6, contextualizes the discussion by providing suggestions for the international community.

---

10 General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, 1 August 2023, paragraph 31(b).

11 All public national positions are available on UNIDIR's Cyber Policy Portal, https://www.cyberpolicyportal.org.

12 General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/79/214, 2 July 2024, paragraph 24.

The categorization of national interpretations as "expansive" or "restrictive" is employed solely for the purposes of analytical clarity of this paper and to illustrate the spectrum of positions. These designations serve as heuristic tools to simplify the discussion and are in no way intended to convey any normative assessment or value judgement regarding the interpretations themselves.

This report offers several benefits, particularly for the United Nations Member States engaged in multilateral discussions on how international law and IHL apply to cyberspace. First, by systematizing and outlining existing national interpretations, the report can function as a reference document for States, supporting their efforts to develop or update national positions on the application of international law, and specifically on IHL, in cyberspace. Indeed, States that wish to develop or update their national position tend to consult or study other States' existing national positions.[13] Second, by outlining outstanding challenges related to the IHL notions of attack and object in the context of digital data, the report can be used as a resource for future discussions aimed at achieving a common understanding on the matter. Both aspects may facilitate the active participation of States in United Nations multilateral discussions on ICTs in the context of international security, including in the permanent Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs, which commenced its work in 2026.[14]

13 UNIDIR Security and Technology Programme, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (Geneva: UNIDIR, 2024), https://unidir.org/publication/a-compendium-of-good-practices-developing-a-national-position-on-the-interpretation-of-international-law-and-state-use-of-ict, 15.

14 General Assembly, resolution 80/16, 1 December 2025.

2. IHL and its principles

One of the main objectives of international law is to foster predictability in international relations. Once an armed conflict begins, IHL aims to limit the effects of armed conflict and to protect persons not participating in hostilities. IHL – the special legal regime governing armed conflict – is premised on the balance between the **two foundational principles of military necessity and humanity**.

The principle of military necessity requires that a party to an armed conflict may only use those means and methods that are necessary to achieve the legitimate purpose of a conflict – that is, "to weaken the military forces of the enemy".[15] The principle does not, however, permit the taking of measures in the name of military necessity that would otherwise be prohibited under IHL.[16] Moreover, a State cannot derogate from a rule of IHL by invoking military necessity unless this possibility is expressly provided for by the rule in question.[17]

The principle of humanity imposes certain limits on the means and methods of warfare and requires that those who have fallen into enemy hands be treated humanely at all times.[18] It seeks to limit suffering, injury and destruction during armed conflict; its purpose is to protect life and health and to ensure respect for fellow humans. It is not allowed, under this principle, to assume that anything that is not explicitly prohibited by specific IHL rules is therefore permitted.[19]

The balance between the two principles of military necessity and humanity is epitomized by the rules for the conduct of hostilities under Additional Protocol I to the 1949 Geneva Conventions.[20] They are comprised mainly by the principles of distinction, proportionality and precaution, and their objective is to protect the civilian population primarily by regulating attacks. These rules are considered to be part of customary IHL, and so must be follow by all States, regardless of whether they are party to Additional Protocol I.[21]

---

15 Saint Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight, 11 December 1868, https://ihl-databases.icrc.org/assets/treaties/130-IHL-6-EN.pdf, preamble.

16 US Military Tribunal at Nuremberg, Hostages case, Judgment, 1948, *The United Nations War Crimes Commission, Law Reports of Trials of War Criminals*, vol. VIII, 1949, pp. 34–76, at 66–67.

17 Yves Sandoz, Christoph Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross (Geneva: Martinus Nijhoff, 1987), paragraph 1389.

18 International Committee of the Red Cross (ICRC), "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts", 32nd International Conference of the Red Cross and Red Crescent, resolution 32IC/15/11, October 2015, https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf, 32.

19 Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (Geneva: ICRC, July 2022), https://shop.icrc.org/download/ebook?sku=4231/002-ebook, 19.

20 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 8 June 1977.

21 See generally Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law* (Cambridge: Cambridge University Press, 2005), https://doi.org/10.1017/CBO9780511804700; International Court of Justice (ICJ, "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion, 8 July 1996, ICJ Report 1996, https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf, paragraph 79.

The principle of **distinction** prohibits parties to a conflict from directly targeting civilians, the civilian population and civilian objects and accordingly requires them to direct their military operations, including attacks, against military objectives only.[22] The principle of proportionality – a corollary of the principle of distinction – prohibits any attack that is expected to cause an amount of incidental civilian harm that would be excessive compared to the concrete and direct military advantage anticipated from an attack.[23] Lastly, the principle of precaution requires those responsible for the planning and execution of an attack to comply with a series of obligations that are essentially aimed at ensuring compliance with the principles of distinction and proportionality and thus to avoid or minimize civilian harm.[24]

These three principles mean that military commanders are subject to the duty to take constant care in the conduct of military operations and to spare the civilian population and civilian objects.[25] They must also do everything feasible to verify that the target of an attack is, in fact, a military objective and not a civilian or a civilian object.[26] Moreover, in the choice of means and methods of warfare, they must do everything feasible to avoid or minimize collateral damage, and they are required to give effective advance warning of incoming attacks if circumstances allow.[27] Finally, they must refrain from launching (or must cancel or postpone) an attack that is reasonably expected to result in excessive collateral damage.[28]

22 Additional Protocol I, Article 48.
23 Additional Protocol I, Article 51(5)(b).
24 Additional Protocol I, Article 57.
25 Additional Protocol I, Article 57(1).
26 Additional Protocol I, Article 57(2)(a)(i).
27 Additional Protocol I, Article 57(2)(a)(ii); Article 57(2)(c).
28 Additional Protocol I, Article 57(2)(a)(iii); Article 57(2)(b).

3. The interpretation of the notion of attack

The term "attack" is defined by Article 49 of Additional Protocol I as an "act of violence against the adversary, whether in offence or defence". The term should be understood as synonymous with "combat action".[29] Accordingly, attacks must comply with all of the rules on the conduct of hostilities: distinction, proportionality and precaution. In contrast, acts that do not amount to "attacks", and which qualify as "military operations", would only be subject to the principle of distinction (so that they can only be directed against military objectives)[30] and are also limited by the duty of constant care.

Conventionally, the notion of violence has been interpreted as being synonymous with "violent consequences" in the form of physical harm: thus, an attack is any act expected to cause death or injury to individuals or damage or destruction to objects (and any combination thereof).[31] To date, few cyber operations on the record have caused physical harm; far more common have been effects such as economic harm or loss of functionality to critical infrastructure, resulting in disruption of essential services. Understandably, the question of which cyber operations qualify as an attack has been the object of significant debate, with two major competing views.

The first approach, which is referred to here as the **restrictive interpretation**, considers that a cyber operation qualifies as an attack when it is "reasonably expected" to cause death or injury to individuals, damage or destruction to objects, or a combination thereof.[32] In this regard, the phrase "reasonably expected to cause" includes any violent consequence that is reasonably foreseeable from the cyber operation.[33]

---

29 Sandoz et al., *Commentary on the Additional Protocols*, paragraph 1880.

30 Certain types of cyber operation (e.g., psychological operations and espionage carried out through cyber means) can, nonetheless, be directed against the civilian population. See Sandoz et al., *Commentary on the Additional Protocols*, paragraph 1875; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rule 63 and accompanying commentary.

31 Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), https://doi.org/10.1017/CBO9781139169288, 107.

32 Schmitt, *Tallinn Manual*, 106. See also Michael Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in *Proceedings of the 4th International Conference on Cyber Conflict*, eds Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 283–93, https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf, 291.

33 Schmitt, *Tallinn Manual*, 107.

The second view, which is referred to here as the **expansive interpretation** and which has been advanced by the International Committee of the Red Cross (ICRC), considers that a cyber operation amounts to an attack when it disables the targeted object "with kinetic or cyber means". This includes also cyber operations that are expected to result in loss of functionality of an object, without necessarily causing physical damage.[34] Notably, the restrictive interpretation does not consider cyber operations that cause loss of functionality as an attack, unless such loss of functionality necessitates replacement of physical components.[35]

The majority of States have yet to express a position on either of the issues presented above. At the time of writing, 24 States have mentioned the notion of "attack" in their national positions. Six of those 24 have adopted an interpretation that could (indirectly) be classified as restrictive, 12 have taken the position classified here as expansive, albeit with varying degrees of nuance. The remaining six have mentioned the notion of "attack" without elaborating further or have acknowledged that the notion of attack deserves further consideration. The following subsections provide further details, focusing on each of the two interpretative schools of thought in turn.

3.1 Notion of attack: restrictive national interpretations

According to the national views that adopt what could be considered a restrictive interpretation, only cyber operations expected to cause physically violent effects can qualify as attacks under IHL. States that have adopted interpretations of the notion of attack labelled here as restrictive have done so with varying degrees of nuance: for example, by stating that a cyber operation constitutes an attack "when the effects of a cyber operation are comparable to those conducted by conventional means or methods of warfare";[36] where "it produces effects similar to those of a kinetic attack";[37] "same or similar to kinetic action that would constitute an attack";[38] or if it "rises to the same threshold of a kinetic attack".[39]

---

34 International Committee of the Red Cross (ICRC), "International Humanitarian Law and Cyber Operations during Armed Conflict: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019", *International Review of the Red Cross*, vol. 102, no. 913 (2020): 481–492, https://doi.org/10.1017/S1816383120000478, 489.

35 Schmitt, *Tallinn Manual*, 108–109. With regards to authors who have adopted an expansive interpretation of the notion of attack, see Giacomo Biggio, "International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber-Attack under Article 49 of Additional Protocol I", *Military Law and the Law of War Review*, vol. 59, no. 1 (2021), 114–140, https://doi.org/10.4337/mllwr.2021.01.06; Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", International Review of the Red Cross, vol. 102, no. 913 (2020): 287–334, https://doi.org/10.1017/S1816383120000387; Ido Kilovaty, "Virtual Violence – Disruptive Cyberspace Operations as 'Attacks' under International Humanitarian Law", *Michigan Telecommunications and Technology Law Review*, vol. 23, no. 1 (2016): 113–151, https://repository.law.umich.edu/mttlr/vol23/iss1/3.

36 Czech Ministry of Foreign Affairs, "Position Paper on the Application of International Law in Cyberspace", 27 February 2024, 10–11.

37 Danish Government, "Denmark's Position Paper on the Application of International Law in Cyberspace", 4 July 2023, 9–10.

38 British Foreign, Commonwealth and Development Office, "Application of International Law to States' Conduct in Cyberspace: UK Statement", 3 June 2021, 7.

39 Australian Government, "Australia's Position on How International Law Applies to State Conduct in Cyberspace" (2017) 2.

One State has specifically stated that is considers a cyber operation as an attack "only if it is expected to cause death or injury to persons or physical damage to objects" or, in other words, "physical damage".[40] According to this State, this view is based on a traditional understanding of IHL and the historical evolution of the notion of attack, which had always been premised on the causation of physical violence.[41]

Two States specifically mention the concept of "loss of functionality" in their national positions. According to one, a cyber operation causing loss of functionality on the targeted computer network or system would only be considered an attack when the loss of functionality is caused by physical damage or when the loss of functionality itself is "a link in a chain of the expected physical damage".[42] That would be the case, for instance, when a cyber operation shutting down the electrical power grid of a military airfield is expected to cause a military aircraft to crash.[43] Another State appears to have endorsed a similar view by stating that it considers a cyber operation as an attack "where it results in death, injury, or physical damage, including loss of functionality, equivalent to that caused by a kinetic attack".[44] In the opinion of the present authors, the reference to loss of functionality "equivalent to that caused by a kinetic attack" refers to permanent and irreversible loss of functionality.

3.2 Notion of attack: expansive national interpretations

Other States advanced a different interpretation of the notion of attack in the context of cyber operations, rejecting the requirement of physical damage as the essential qualifier of the notion of attack. Views expressed by these States – subscribing to what is classified hare as an expansive interpretative approach – are not uniform, and there is a certain degree of nuance provided by individual national positions.

Thus, one State has argued (using words similar to those employed by the ICRC) that a cyber operation "may constitute an attack under IHL" if it is "designed to disable, either in a kinetic or non-kinetic context, an ICT network of the adversary during an armed conflict".[45]

The national position of another State explicitly clarifies that that the notion of cyberattack is not characterized solely on the basis of material criteria.[46] According to that State, a cyber operation qualifies "as an attack when the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not".[47] Another State has emphasized that that "the occurrence of physical violence, injury or death to persons or damage

40 Roy Schöndorf, Israeli Ministry of Justice, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, vol 97 (2021): 399–401, https://digital-commons.usnwc.edu/ils/vol97/iss1/21, 395.

41 Schöndorf, "Israel's Perspective".

42 Schöndorf, "Israel's Perspective".

43 Schöndorf, "Israel's Perspective".

44 New Zealand Government, "The Application of International Law to State Activity in Cyberspace", 1 December 2020, 4.

45 Austrian Government, "Cyber Activities and International Law", Position Paper, April 2024, 17.

46 French Ministry of Defence, "International Law Applied to Operations in Cyberspace", 9 September 2019, 13. Similarly, see Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position on the Application of International Law in Cyberspace", 21 July 2023, 13.

47 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", 8.

or destruction to objects comparable to effects of conventional weapons, is not required for an attack in the sense of Art. 49 [of] Additional Protocol I".[48] According to this interpretation, a cyber operation qualifying as an attack under IHL is an operation harming communications, information or other electronic systems, as well as any information that is stored, processed or transmitted on these systems.[49]

Another State has adopted an interpretation of the notion of cyberattack that focuses on the effects of cyber operations on critical infrastructure.[50] Although States have not adopted a common definition of critical infrastructure, the concept could include, and is not limited to, sectors like healthcare, transportation, energy, banking and finance, civilian logistical supply chains, and undersea fibre-optic cables, satellites, and other telecommunications networks. In the view of this State, a cyber operation would qualify as an attack if it attempts to delete, destroy and manipulate the data essential for the smooth functioning of a critical infrastructure, undermining the confidentiality, integrity and availability of that data.[51] Accordingly, disabling the ICT network of a critical infrastructure may have reverberating effects that undermine the functioning of the State as a whole or its critical national interests.[52]

Moreover, some of the States endorsing the expansive interpretation of attack have mentioned the concept of "loss of functionality" in their national positions.[53] One State in particular refers to "loss of functionality to medical institutions" as an example of a cyber operation qualifying as an attack under the IHL.[54] Another State has taken the view that a cyber operation that encrypts data through a ransomware attack could qualify as an attack.[55]

---

48 German Government, "On the Application of International Law in Cyberspace", Position Paper, March 2021, 8.

49 German Government, Position Paper.

50 Pakistani Government, "Pakistan's Position on the Application of International Law in Cyberspace", 3 March 2023, paragraph 14.

51 Pakistani Government, "Pakistan's Position".

52 Austrian Government, Position Paper, 17.

53 Colombian Ministry of Foreign Affairs, "Colombia's National Position on the Application of International Law in Cyberspace", 2025, 12–13; Irish Department of Foreign Affairs, "Position Paper on the Application of International Law in Cyberspace", 6 July 2023; Slovenian Ministry of Foreign and European Affairs, "Slovenia's Position Paper on the Importance of International Law in Cyberspace", April 2025, 6.

54 Japanese Ministry of Foreign Affairs, "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations", 28 May 2021, 7.

55 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", 13.

4. Digital data as objects under IHL

Closely related to the definition of attack in the cyber domain is the question of whether digital data qualify as an object under IHL. Under the restrictive interpretation, the term "object" is connected to the definition of attack under Article 49 of Additional Protocol I since violence (the essential prerequisite by which an act qualifies as an attack) generally includes damage or destruction of objects. If digital data qualifies as an object under IHL, then cyber operations that delete, alter or interfere with data would qualify as attacks and, accordingly, would need to comply with applicable IHL rules on the conduct of hostilities. Moreover, the term object is essential for the application of the principle of distinction, which requires belligerents to distinguish at all times between civilian objects and military objectives. Accordingly, if data is considered as an object, then it should be considered as protected from direct attack unless it qualifies as a military objective. It may also benefit from the protection offered by specific provisions of IHL to certain categories of object, such as objects indispensable for the survival of the civilian population, medical services and humanitarian relief operations.[56]

The debate on the issue of data under IHL shares some similarities with that on the definition of attack. Specifically, the proponents of what could be considered as restrictive interpretations do not consider that digital data falls within the ordinary meaning of the term object[57]– the latter notion is taken to include only entities that are both tangible and visible, two qualities that data does not possess.[58] At the other end of the interpretive spectrum, among those taking what can labelled as an expansive interpretation, the ICRC has argued that, "[w]hile the question of whether and to what extent civilian data constitute civilian objects remains unresolved",[59] it would run contrary to the object and purpose of IHL to not prohibit a cyber operation that deletes or tampers with essential civilian data (e.g., medical data, biometric data, social security data, tax records, bank accounts, companies' client files, or election lists and records).[60] Therefore, "[e]xcluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap".[61]

---

56 Gisel et al., "Twenty Years On", 327–329.

57 Schmitt, *Tallinn Manual*, 407–408. See also Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law", *Journal of Conflict and Security Law*, vol. 28, no. 2 (2023): 349–387.

58 Sandoz et al., *Commentary on the Additional Protocols*, paragraph 2008.

59 International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflict", 490.

60 International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflict".

61 International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflict". With regards to scholars who have adopted an expansive interpretation, see Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, vol. 48, no. 1 (2015): 39–54, https://doi.org/10.1017/S0021223714000272; Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, vol. 48, no. 1 (2015): 55–80, https://doi.org/10.1017/S0021223714000260.

With regards to the question of whether digital data qualifies as an object, only 11 States have expressed their interpretative positions on the matter. Among those, only two hold the view that digital data is not an object, thus aligning themselves with the scholarship arguing for a restrictive interpretation; seven of them have endorsed an expansive interpretation of the notion of "object" under IHL, seemingly sharing the concern expressed by the ICRC; and two acknowledge that the question related to the status of data under IHL requires further consideration.

4.1 Digital data: restrictive national interpretations

States that have adopted what could be considered a restrictive interpretation of the notion of data hold the view that, for the purposes of IHL, objects have traditionally been understood to be visible and tangible things. According to those States, it follows that, since data is not visible or tangible, it does not fall within the ordinary meaning of the notion of object under IHL.[62] Having said that, these States consider that a cyber operation against data may nonetheless qualify as an attack if it may foreseeably result in adverse effects on individuals or physical objects.[63]

4.2 Digital data: expansive national interpretations

An assessment of the national positions of those States that regard digital data as an object reveals varying degrees of nuance, very much like that noted in Subsection 3.2 in relation to the notion of attack.[64] For example, these States argue that data is to be considered an object for the rules governing the conduct of hostilities, in particular the principle of distinction.[65] Some States hold the view that data, as a civilian object, is protected from attack unless it becomes a military objective.[66] One State, in particular, has stated that civilian data sets (e.g., medical data, bank data, social security data, tax records, and corporate and financial data) must be protected, since they are considered to be critical components of digitalized society and play a vital role in the functioning of many aspects of civilian life.[67]

62 Schöndorf, "Israel's Perspective", 400.
63 Danish Government, "Denmark's Position Paper", 10.
64 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", 13–14.
65 French Ministry of Defence, "International Law Applied to Operations in Cyberspace", 14; German Government, Position Paper, 8.
66 Austrian Government, Position Paper, 18; Colombian Ministry of Foreign Affairs, "Colombia's National Position", 11.
67 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", 13–14.

5. Practical implications

To illustrate the practical implications of legal differences between the expansive and restrictive approaches to the interpretations of the notions of attack and data, the following subsections discuss two hypothetical scenarios in which a data centre is targeted by a malicious cyber operation. A data centre is defined here as "a physical facility that houses computer systems; networking equipment; and associated components for the purposes of storing, processing, and disseminating data and applications".[68]

5.1 Scenario 1: A cyber operation resulting in physical damage

In the first fictional scenario, members of the armed forces of a State engaged in an international armed conflict plan to deploy a wiper malware targeting the supervisory control and data-acquisition (SCADA) system of a power grid that provides electricity to a pair of data centres: one data centre hosts applications used by the military to conduct weapon simulations as well as simulations of hostilities in an ongoing armed conflict; and the other hosts civilian applications and stores social security data. The deployment of the malware is expected to cause a catastrophic failure within each data centres' own power infrastructures, and result in fires that could damage or destroy the buildings housing the computer systems and servers.

Under both the **restrictive and expansive** interpretations of an attack under the IHL, the cyber operation would qualify as an attack since it is reasonably expected to cause physical, violent effects in the form of damage and destruction of objects.

Where the two approaches differ is in relation to assessing whether the cyber operation complies with the principles of distinction, proportionality and precaution. The application of these principles would depend on the interpretation of the notion of data, resulting in different targeting obligations and practical outcomes.

5.1.1 The principle of distinction

With regards to the principle of distinction, it is worth re-emphasizing that Article 48 of Additional Protocol I requires parties to a conflict to direct their military operations (including attacks) against military objectives only, whereas Article 52 of Additional Protocol I provides that civilian objects shall not be made the object of attack and that attacks shall be limited strictly to military objectives.[69] In turn, military objectives are defined as "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".[70]

---

68 François Delerue, "Data Centers and International Humanitarian Law", in *Big Data and Armed Conflict: Legal Issues Above and Beyond the Armed Conflict Threshold*, eds Laura Dickinson and Edward Berg (Oxford: Oxford University Press, 2023), 207–227, https://doi.org/10.1093/oso/9780197668610.003.0009, 209.

69 Additional Protocol I, Article 52.

70 Additional Protocol I, Article 52(2). See also Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Rule 1.

Under the **restrictive** interpretation of the notion of data, the applications used by the military would not be considered as an object and would therefore not qualify as a military objective. Only the computer systems that operate these applications, the servers where the applications are stored and the building where the data centre as a whole is located could potentially qualify as a military objective, provided that they satisfy the requirements laid down in Article 52 of Additional Protocol I.

Conversely, under the **expansive** interpretation of the notion of data, the data stored in the servers as well as the applications would be considered as objects. However, only the data and applications that make an effective contribution to military action, and whose destruction would offer a definite military advantage, would qualify as a military objective and thus legitimate targets under IHL. Conversely, civilian data and applications cannot be directly made the object of an "attack" – should that be the case, this would violate the principle of distinction and would amount to a grave breach of IHL.

Therefore, depending on the interpretation that is given to "data", the resulting definition of military objective will be either less specific (under the restrictive interpretation) or more specific (under the expansive interpretation).

5.1.2 The principle of proportionality

With regards to the principle of proportionality, Article 51(5)(b) of Additional Protocol I prohibits any attack that is expected to cause an amount of incidental civilian harm that is excessive compared to the concrete and direct military advantage anticipated. The notion of incidental harm comprises "death, injury to individuals, damage or destruction to objects, or a combination thereof".

Under the **restrictive** interpretation of data, the incidental harm to be accounted for in an assessment of proportionality would be limited to any damage caused to the physical structure of the data centre as a whole, including the servers and the computer networks.

Conversely, under the **expansive** interpretation, the assessment of collateral damage would also include any destruction of civilian data and applications that are stored and processed in the data centre. Under the expansive interpretation, this destruction would constitute a subset of the category of damage or destruction to civilian objects. Such civilian data may serve essential functions related to, for example, the healthcare or energy industries, and deleting or altering it may have severe adverse effects on the sectors that rely on them.

Therefore, and as far as the principle of proportionality is concerned, the scope of collateral damage that would have to be considered under the expansive interpretation would be greater than under the restrictive interpretation since the former would include any collateral damage or destruction of civilian data, while the latter would not.

5.1.3 The principle of precaution in attack

With regards to the principle of precaution in attack, two obligations are particularly relevant to this scenario. First, in choosing means and methods of warfare, those who plan or decide on an attack must do everything feasible to avoid or minimize incidental civilian harm, injury to civilians or damage to civilian objects. Second, they must refrain from launching (or must cancel or postpone) an attack that is reasonably expected to result in excessive incidental harm.[71]

Under the **restrictive** interpretation, the notion of incidental harm would not include any damage, corruption or alteration to digital data. In contrast, this type of damage would have to be considered under the **expansive** interpretation.

5.2 Scenario 2: A cyber operation causing loss of functionality and data deletion but not resulting in physical damage

Now consider the same scenario – deploying a wiper malware targeting the SCADA system of a power grid that is reasonably expected to delete data – but where it is reasonably expected that no physical damage will be caused.

Under the **restrictive** interpretation of the notion of attack, the operation would not qualify as an attack and would therefore not be subject to all the rules stemming from the three principles of IHL since no death or injury to individuals or damage or destruction to objects can be reasonably expected from the attack. In addition, deleting data would not be considered as destruction of objects since, under the restrictive interpretation, data falls outside the ordinary meaning of the term. Accordingly, the cyber operation would not be limited by the rules on the conduct of hostilities related to the principles of distinction, proportionality and precaution. However, it would still be subject to the duty, incumbent on military commanders under Article 57 of Additional Protocol I, to "take constant care, in the conduct of military operations, to spare the civilian population and civilian objects", as well as potentially other special protections under IHL.

Conversely, under the **expansive** interpretation of the notions of attack and data, the cyber operation would qualify as an attack because it could reasonably be expected to delete data, thereby causing damage to objects. The operation would therefore have to comply with the principles of distinction, proportionality and precaution.

71 Additional Protocol I, Article 57(2)(a)(iii); Article 57(2)(b).

5.2.1 The principle of distinction

As stated above, the principle of distinction prohibits the attacker from directly targeting civilian objects. The only digital data and applications that would qualify as a military objective are those that make an effective contribution to military action and whose destruction or neutralization would offer a definite military advantage in the circumstances ruling at the time. Moreover, the cyber operation would have to comply with the prohibition on indiscriminate attacks enshrined under Article 51(4) of Additional Protocol I, which prohibits "attacks that are not directed against a specific military objective" (Article 51(4)(a)), "attacks which employ a means or method of warfare which cannot be directed at a specific military objective" (Article 51(4)(b)), and "attacks which employ a means or method of warfare the effects of which cannot be limited as required by the Protocol" (Article 51(4)(c)).

For the present purposes, this would mean that the cyber operation would be considered as an indiscriminate attack in violation of IHL if it were to employ a technique that makes no distinction between civilian data and data used for military purposes, such as a wiper malware that spreads uncontrollably across data sets and application within the data centres.

5.2.2 The principle of proportionality

If the cyber operation complies with the principle of distinction, it must also respect the principle of proportionality. Similarly to scenario 1, the expected collateral damage to be accounted for in the proportionality assessment would include any damage or destruction to civilian data sets and applications. If the expected incidental damage would be excessive in relation to the anticipated concrete and direct military advantage, the operation would be considered a disproportionate attack, thus resulting in a grave breach of IHL.

5.2.3 The principle of precaution in attack

With regard to the principle of precaution in attack, Article 57(3) of Additional Protocol I is particularly significant for this scenario since it provides that, "when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects".

Under the **expansive** interpretation of the notion of data, this would mean that the attacker must choose between different military objectives, provided that they would result in a similar military advantage: either the physical structure of the data centre, its computers and servers; or the data and applications that are stored and processed in the data centre. The attacker may therefore be required to select a cyber operation that only affects data if this would result in the least amount of danger to civilian lives and civilian objects.

6. Conclusions and recommendations

As demonstrated here, there is currently no common understanding of how IHL applies to cyberspace. The divergence in national interpretations of the notions of attack and digital data leads to different legal assessments of cyber operations in the context of an armed conflict, particularly those causing loss of functionality or data deletion in the absence of physical harm.

The absence of a common understanding of what constitutes permissible – or impermissible – behaviour in an armed conflict augmented by ICT activity is not merely an academic concern; it is a pressing practical issue with potential real-world consequences in the context of current or future armed conflicts. Lack of legal clarity reduces the predictability of the use of ICTs on the battlefields and hampers the potential of IHL to protect the civilian population or civilian objects.

It should be noted, however, that uniform and universal common understanding of the existing international law and international (humanitarian) law is unlikely given that interpretative divergences are not unusual and exist even in respect to rules and principles considered to be foundational to the contemporary legal regimes supporting international peace and security. However, **seeking common understanding of how IHL applies to cyberspace can nevertheless provide greater clarity on international limits on the use of ICTs in an armed conflict. This, in turn, would increase the predictability of international relations and establish clear safeguards for civilians and civilian objects**.

To contribute to legal clarity and alleviate the challenges identified above, States could continue seeking common understanding of how IHL applies to cyberspace in an armed conflict through **collective or individual abstract interpretative efforts as well as by sharing outcomes of practical legal analyses of fictional or observed use of ICTs in the contexts of armed conflicts**. As emphasized by this paper, some of the main questions in need of further clarity are whether loss of functionality of an ICT system is considered an attack under IHL and whether digital data enjoys legal protection as an object under the current normative regime.

From 2026, there is a new forum in which collective theoretical efforts can be made towards common understanding of how international law and IHL apply to cyberspace: the Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs. The new Global Mechanism is a permanent, single-track multilateral

process under the auspices of the United Nations that is set to "continue to study how international law applies in the use of ICTs… and to consider whether any gaps exist in how existing international law applies in the use of ICTs and further consider the development of additional legally binding obligations", among other things.[72] International law and IHL are also to feature in the working group discussions of the Global Mechanism.[73] States could consider **active and substantive engagement in the discussions of the Global Mechanism**.

States can also contribute to building a common understanding of how international law and IHL apply to cyberspace through **publication of individual national interpretative positions and reports of State practice**. Indeed, in the final report of the OEWG 2021–2025, States "strongly encouraged" such practice.[74] To maximize the contribution of national positions to transparency and legal clarity, States could consider publishing their national positions on, for instance, the websites of the relevant government entities, on the websites of the relevant multilateral processes, or even in law journals and dedicated confidence-building platforms such as Cyber Policy Portal.[75] Domestically, States could consider incorporating their interpretative views in various relevant national governance frameworks, including, for instance, in military manuals or perhaps even cybersecurity strategies.

States could also contribute to common understanding of how international law applies to cyberspace by applying theoretical national interpretations to fictional or real examples of the use of ICTs in the context of armed conflicts – much like the scenarios in Section 5 above. **Legal analysis of practical examples of cyber operations can translate abstract legal concepts into concrete scenarios and can promote inclusive engagement of the multi-stakeholder community – beyond legal professionals in diplomatic efforts – on the use of ICTs in the context of international security**. This could take place, for example, in the Global Mechanism.

The underlying enabler of contributions to the efforts seeking convergence on a common understanding of how IHL applies to cyberspace is capacity-building.[76] **Politically neutral, sustainable, objective and sovereignty-respecting capacity-building, including withing the United Nations, remains essential for inclusive and diverse set of national contributions to common understanding**.[77]

---

72 General Assembly, A/79/214. See also General Assembly, "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security", Report of the Secretary-General, A/78/76, 18 April 2023, paragraph 29; "[Draft] Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security, Rev. 2, 18 June 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_18_June_2024.pdf, paragraph 14.

73 General Assembly, A/80/257, Annex I, paragraph 7 referring to "all pillars", which includes international law and IHL.

74 General Assembly, A/80/257, paragraph 43(b).

75 As recommended by the OEWG 2021 consensus report. General Assembly, A/75/816, paragraph 50. See also General Assembly, A/75/816, Annex II, "Chair's Summary", paragraph 19. See, in general, UNIDIR Security and Technology Programme, *A Compendium of Good Practices*, ss2.

76 General Assembly, A/80/257, paragraph 43(d).

77 General Assembly, A/75/816, paragraph 56; General Assembly, A/80/257, paragraph 43(d).

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG