BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 17, NUMBER 1 (2024)
ISSN 2029-0454

Cit.: *Baltic Journal of Law & Politics* 17:1 (2024): 1–20
https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml
DOI: 10.2478/bjlp-2024-0001

PROTECTION OF (PERSONAL) DATA IN ARMED CONFLICTS

Bence Kis Kelemen
PhD, senior lecturer
University of Pécs, Hungary

Contact information:
Phone: +36 70 501 599 23237
E-mail: kis.kelemen.bence@ajk.pte.hu

Received: September 6, 2023; reviews 2; accepted: January 10, 2024.

ABSTRACT

Despite the increased attention that was given to data protection laws in national jurisdictions – especially after the adoption of the General Data Protection Regulation by the European Union – international law still does not offer a higher standard of protection to the personal data of civilians in times of armed conflict, where the deletion or manipulation of personal data of the civilian population can have significant harmful effects. This article explains that at the time of the adoption of the relevant international treaties and the development of customary international law, international humanitarian law (IHL) did not protect personal data stored electronically, and even though commentators in contemporary times tend to accept the object status of electronic data, State practice still remains inconclusive, largely excluding computerized personal data from the protective regime of IHL. The article argues further that a stricter protection of personal data regulation could potentially lead to harmful effects for protected persons, such as civilians, therefore it is undesirable. The protective nature of IHL must prevail over the data protection interests.

KEYWORDS

Personal data, object, IHL, cyberspace, civilian, cyber operation.

INTRODUCTORY REMARKS[1]

The protection of personal data has gained significant attention in recent years. For instance, the European Union has re-regulated the issue by Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). By its very nature, this and similar laws do not apply in times of armed conflict. This is highlighted in the GDPR, for example, by stating that the regulation does not apply in activities falling outside the scope of EU law and in the area of the Common Foreign and Security Policy.[2] However, as Robin Geiß and Henning Lahmann argue, GDPR and other existing data protection and security legal frameworks can serve as a novel starting point for discussing prominent data related international humanitarian law (IHL) questions.[3] This article aims at connecting personal data protection as understood in the GDPR with protection of (personal) data under IHL as set out below.

We are increasingly dependent on various computer systems and the internet, which inevitably contain and use our personal data. Such personal data exists essentially in computerized form, namely, as electronic or computer data. Computer data is best defined as information that is handled or stored via computers.[4] In light of the above, it is not surprising that the International Committee of the Red Cross (ICRC) has concluded that cyber-attacks can lead to dramatic humanitarian consequences and that even operations that do not cause death or injury directly – such as the disruption of the banking system – can have serious ramifications.[5]

Such cases inevitably raise the question: what legislation governs those operations and thus the protection of personal data in the event of armed conflicts from the perspective of IHL? First, there is consensus in the international community that international law applies in cyberspace,[6] but not all States agree on the application of IHL.[7] For instance, Russia claimed that applying the law of armed conflict in the cyber context would contribute to the militarization of cyberspace, and furthermore IHL is not fit to govern new tools such as the information and communication technology (ICT).[8] Similar views were advanced by Iran[9] and Cuba.[10] China on the other hand smees to accept

1 Supported by the ÚNKP-21-4-I New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund, and supported by the ÚNKP-22-4 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund. The article builds on a similar article of the author published in Hungarian: Bence Kis Kelemen: "Személyes adatok védelme fegyveres konfliktusokban," *Jogtudományi Közlöny* 77 (2022): 395–402.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal (2016, no. L 119), art. 2, para. 2 (a)-(b). (hereinafter: GDPR).

3 Robin Geiß and Henning Lahmann, "Protection of Data in Armed Conflict," *International Law Studies* 97 (2021): 556–559.

4 Ibid.

5 ICRC, *International humanitarian law and the challenges of contemporary armed conflicts report* (Geneva: International Committee of the Red Cross, 2015), 32IC/15/11, 39 (hereinafter: 32IC/15/11).

6 UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 June 2013), UN Doc A/68/98, para 19.

7 Kubo Mačák, "This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace," *Exeter Centre for International Law Working Paper Series* 2/2019 (2019): 3; Dapo Akende, Antonio Coco and Talita de Souza Dias, "Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies," *International Law Studies* 99 (2022): 6–7.

8 Liina Lumiste, "Russian Approaches to Regulation Use of Force in Cyberspace," *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 125 // DOI:10.1163/22115897_02001_007

9 Tal Mimran, "Between Israel and Iran: Middle-East Attitudes to the Role of International Law in the Cyber-Sphere," *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 219 // DOI: 10.1163/22115897_02001_011

10 Representaciones Diplomáticas de Cuba en El Exterior, *71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context*

the applicability of IHL to cyber operations, at least when it comes to the fundamental norms of the field. Additionally, China emphasizes the need for further IHL norms to fully regulate the field.[11] To circumvent the alleged factors precluding the applicability of the law of armed conflict in the ICT context, reference needs to be made to the Advisory Opinion rendered by the International Court of Justice in the Nuclear Weapons case. In their decision, the judges opined that IHL should be applied to past, present, and future weapons alike, meaning that although nuclear weapons were non-existent when the fundamentals of IHL have been formulated, this does not affect the applicability of its principles to the use of such technology.[12] The same arguments can be brought in support of the applicability of IHL to cyberspace.[13] Furthermore, merely regulating an issue does not correspond to legitimizing or even justifying the conduct in question.[14] A simple reference can be made to the prohibition on the use of force and the connected *jus contra bellum* regime, which gives States the possibility to use interstate force only in very narrow circumstances, for example in self-defense. But in no way does this encourage members of the international community to start conflicts. In addition, international legal scholarship also accepts this position as affirmed by Rule 80 of the Tallinn Manual 2.0.[15] Given the above considerations, and the fact that most States accept the application of the law of armed conflict to the information space, this article examines the protection of personal data through the lens of IHL.

This approach – in other words, IHL as the interpretive background of this analysis – is without prejudice to other fields of international law applicable to the protection of personal data in times of armed conflict, such as international human rights law. As noted by the International Court of Justice, human rights law may be applicable within the framework of an armed conflict as well, subject to derogations and *lex specialis* IHL norms relating for example to right to life.[16] The relevant human right for the protection of personal data is the right to privacy enshrined in a number of international treaties, for instance the International Covenant on Civil and Political Rights,[17] and the European Convention on Human Rights[18] and other international instruments.[19] The right to privacy – containing the protection of personal data – is not an absolute right; therefore, it can be subjected to limitations and derogations.[20] As the GDPR is a modern standard

of international security (June 2017) // https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information. Cuba claimed that such as view would "legitimize an scenario of war and military actions in the context of ICT".

11 Lixin Zhu and Wei Chen, "Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Coexistance," *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 197–198 // DOI: doi.org/10.1163/22115897_02001_010. It needs to be noted, that this article serves more like a propagandistic public policy program from China, than a scientific work.

12 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226, para 86.

13 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 (January 2015): 71 // DOI: doi.org/10.1017/S0021223714000260

14 Kubo Mačák, *supra* note 6, 3.

15 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 375.

16 Legality of the Threat or Use of Nuclear Weapons, *supra* note 11, para 25.

17 *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976), 999 UNTS 171 (ICCPR), art. 17.

18 *Convention for the Protection of Human Rights and Fundamental Freedoms* (adopted 4 November 1950, entered into force 3 September 1953), ETS 005, art. 8.

19 See also *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (adopted 28 January 1981, entered into force 1 October 1985), ETS 108.

20 Eliza Watt, *State Sponsored Cyber Surveillance. The Right to Privacy of Communications and International Law* (London: Edward Elgar, 2021) 193, 196.

or manifestation of the protection of personal data as a standalone human right,[21] it is perfect candidate for determining whether a personal data protection regime is warranted in times of armed conflict, or not; in other words, whether GDPR or other similar national data protection laws have something to offer when it comes to developing international law applicable in times of armed conflict.[22]

The article first examines whether personal data stored electronically can be considered an object under the law of armed conflict, and to a limited extent, whether military operations against personal data can be considered an attack as defined by IHL based on interpretation of the applicable law and a review of the relevant works of international legal scholars. As both 'attack' and 'objects' are inherent terms of IHL, the article will get back on them in detail. The basis of this investigation is twofold. On the one hand, the GDPR regulates the processing of personal data wholly or partly by automated means,[23] thus electronically. On the other hand, there is an intensive discussion in academia and in State practice, whether electronic data – regardless of whether it can also be considered personal data or not – should enjoy the protection afforded to civilian objects. The article aims to connect these problems and investigate the status of electronically stored personal data in the context of an armed conflict, from the perspective of IHL (Part II). The article then points out, on the basis of an analysis of State practice, that while current State practice undoubtedly shows a shift towards the object status of civil data and thus personal data, there is not yet sufficient practice to depart from the original interpretation of the treaties and customary international law (Part III). The article concludes that despite the identifiable trend in both scholarship and State practice, electronically stored data in general and as an extension, personal data is not protected as civilian objects, despite the convincing policy considerations for such an interpretation of existing law. Finally, the article argues that the application additional norms, such as for example the principles of GDPR for the protection of personal data is neither possible nor desirable in an armed conflict, using the example of data-intensive military operations, such as targeted killings (Part IV).

1. IS PERSONAL DATA STORED ELECTRONICALLY CONSIDERED AN OBJECT UNDER IHL?

In order to determine whether personal data, notably electronic personal data within the framework of this article, constitute objects in the law of armed conflicts, it is appropriate to define the notion. The concept of personal data is not defined in IHL, so it is logical to rely on the GDPR, which defines personal data as

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[24]

---

[21] *Charter of Fundamental Rights of the European Union* (adopted 7 December 2000, entered into force 1 December 2009), OJ C 326, art. 8.

[22] The framing here is intentional, as it refers to the fact, that not only IHL but international human rights law can be applicable in armed conflict and a personal data protection regime can be understood from the perspective of both fields of law.

[23] GDPR, *supra* note 1, art. 2, para 1.

[24] GDPR, *supra* note 1, art. 4, para 1.

On the other hand, as far as objects are concerned, one can find a treaty based starting point in IHL, which distinguishes between military objectives and civilian objects. Military objectives are "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".[25] In comparison, civilian objects are those which do not constitute military objectives as defined above.[26] These concepts also have the same meaning in customary international law.[27]

On that basis, electronically stored personal data can be classified as a military objective, or as a civilian object if it is regarded as an object. The ICRC commentary of the Additional Protocol I to the 1949 Geneva Conventions from 1987 states on this issue, that an object must be a visible and tangible thing, which applies for objectives as well.[28] At the time of the adoption of the treaty therefore, objects were tangible and visible in the traditional sense. Since electronic data, thus personal data stored in computerized form, is not of such nature, they did not constitute it as an object at that time.

In light of the current state of the art, and the time that has elapsed since the concept was created, it is not surprising that the legal literature is divided on the question of whether or not computer data may be classified as objects. The Tallinn Manual 2.0, adopted as a private codification effort, is an excellent starting point for understanding the position of commentators, which sets out the professional views of the experts involved in its creation on international law applicable to cyberspace.[29]

Rule 100 of the Tallinn Manual deals with civilian objects and military objectives practically the same way as Additional Protocol I. The former highlights that cyber infrastructure, such as communication, computing and storage devices on which information systems are built and operated[30] can serve as a military objective.[31] The Tallinn Manual then provides examples of objects in cyber warfare, such as a computer or their network and some tangible elements of cyber infrastructure; however, it emphasizes, that messages, although they may be used for military operations, are not objects or military objectives.[32]

The Tallinn Manual also provided a detailed position on the object status of electronic data. The majority of experts involved in the private codification process took the view that data should not be considered objects, as among others, they are not tangible nor visible.[33] A minority of experts, on the other hand, argued that as a minimum data necessary for the well-being of the civilian population was, in any event, a civilian object, such as data relating to social security, tax information, banking data, etc.[34] Each

---

25 *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I)* (adopted 8 June 1977, entered into force 7 December 1979), UNTS 1125 3, art. 52, para 2 (hereinafter: Additional Protocol I).

26 *Ibid.,* art. 52, para 1. This definition of military targets and thus of objects is linked to the name of the German nationaž Friedrich August Freiherr von der Heydte Baro, who created that concept as a rapporter of the Institute of International Law, which was adopted in 1969 as a description of the law in force. See Eyal Benvenisti, "The Birth and Life of the Definition of Military Objectives," *International & Comparative Law Quarterly* Vol. 71, No. 2 (May 2022): 269, 279, 285, 289 // DOI: doi.org/10.1017/S0020589322000100

27 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law – Volume I: Rules* (New York: International Committee of the Red Cross – Cambridge University Press, 2005), 29, 34.

28 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: International Committee of the Red Cross, 1987), 633–634.

29 Michael N. Schmitt, *supra* note 14, 2.

30 *Ibid.,* 564.

31 *Ibid.,* 435–436.

32 *Ibid.,* 436–437.

33 *Ibid.,* 437.

34 *Ibid*.

and every one of these categories of data coincides with personal data as defined by the GDPR.

Apart from the Tallinn Manual, international legal scholarship on IHL applicable in the cyber context often does not contribute to this debate in a meaningful manner, as it merely reiterates the content of the Tallinn Manual or does not mention this problem at all.[35]

However, some authors have taken a clear position in the debate. For example, Terry D. Gill approaches the problem through the notion of attacks and argues that, under current international law, cyber operations against data do not qualify as an attack under IHL.[36] As will be shown below, an attack can only be directed against objects. Michael N. Schmitt also supports the Tallinn majority position on this issue, arguing among others that *lex lata* the object status of electronic data cannot be supported.[37] He contends that the object status of data can be over- and underinclusive at the same time.[38] Schmitt also argues as a policy proposal that special protection should be granted to essential civilian services and functions, as well as financial data. Furthermore, a proportionality test should be introduced for operations similar to that, which is applicable to an attack.[39] In the same vein, Ori Pomson asserts, that according to current customary international law, objects are material things,[40] and claiming otherwise would cause serious repercussions. According to the author, computer data are merely binary signals, which do not exist in tangible form, and even scrolling can change data. This means, that *ad absurdum* scrolling through this article could also be seen as an attack under IHL, if one would consider electronic data to be objects.[41]

In contrast, other authors such as Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann claim that certain personal data, for instance medical data enjoy special protection and emphasize the ICRC's supporting position for the object status of electronic data due to the their significance in the lives of societies.[42] Tim McCormack and Kubo

---

35 See *e.g.* Yuval Shany and Tal Mimran, "International Regulation of Cyber Operations," *Hebrew University of Jerusalem Legal Studies Research Paper Series* 5/2021 (November 2021): 16; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Cambridge: Cambridge University Press, 2014), 183–184. According to the author, the question does not need to be over-dimensioned, since, based on the term used by the author to attack, an operation involving data is classified as an attack only in the event of a physical consequence to the operation, therefore, the status of data is irrelevant; Christopher S. Yoo, "Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures": 186; in: Jens David Ohlin, Kevin Govern and Claire Finkelstein, eds., *Cyberwar. Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press, 2015). The author mentions only attacks on data characterized by the Tallinn Manual; Kriangsak Kittichaisaree*, Public International Law of Cyberspace* (Cham: Springer, 2017), 205–207, 211. The author presents the views of the Tallinn Manual and the ICRC on attacks against data and the ICRC's views on medical data; William H. Boothby, "Cyber Capabilities": 95; in: William H. Boothby, ed., *New Technologies and the Law in War and Peace* (Cambridge: Cambridge University Press, 2019). The author does not even mention the issue, except touching upon it in relation to cyber espionage causing physical damage.

36 Terry D. Gill, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict": 466; in: Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2021).

37 Michael N. Schmitt, "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision," *Israel Law Review* Vol. 48, No. 1 (March 2015): 81, 87 // DOI: doi.org/10.1017/S0021223714000314

38 Michael N. Schmitt, "Wired warfare 3.0: Protecting the civilian population during cyber operations," *International Review of Red Cross* Vol. 101, No. 1 (April 2019): 333, 342 // DOI:10.1017/S1816383119000018

39 *Ibid.,* 345–347; Michael N. Schmitt, "International cyber norms: reflections on the path ahead," *Netherlands Military Law Review* 111 (2018): 12, 21; It author also warrants special protection to certain data based on special protection norms. See Michael N. Schmitt, *supra* note 36, 106.

40 Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law," *Journal of Conflict & Security Law* Vol. 28, No. 2 (January 2023): 38 // DOI: doi.org/10.1093/jcsl/krad002.

41 *Ibid.,* 4–5.

42 Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty years on: International humanitarian law and the protection of civilians against effects of cyber operations during armed conflicts," *International*

Mačák go even beyond that, arguing that *lex lata* IHL extends the object status to electronic data.[43] Similarly, Noam Lubell asserts that the interpretation of data as objects is closer to the intention of the founding fathers of IHL.[44] In the same vein, Kubo Mačák argues that the ordinary meaning of the term 'object' has changed in recent years, which now includes electronic data.[45] Another proponent of the object status of data is Heather A. Harrison Dinniss, who differentiates between content-level and operational-level data. Where the former includes texts, images etc*.,* the latter is considered to be the program data, or code. According to Harrison Dinniss, although content-level data – including personal data – may be considered an object, they are mainly subject to special protection, such as medical data.[46] Her main argument is that operational-level data should be considered an object.[47] Similarly, the Global Advisory Board on Digital Threats during Armed Conflicts also claims, that the category of civilian objects include data.[48] This Board is comprised of experts in the field including Dapo Akande.[49]

Although it is highly debated among experts whether computer data may be regarded as an object under IHL, the number of commentators who are in favor of an affirmative answer has increased significantly in recent years.

In addition, reference should be made to the link between the notions of attack and object. Article 49(1) of Additional Protocol I defines the term attack as "acts of violence against the adversary, whether in offence or in defence".[50] In contrast, customary international law does not define the concept of an attack unlike it did with military objectives and civilian objects.

The commentary to the Additional Protocol I notes in relation to attack that it must be a combat action.[51] The Tallinn Manual states that cyber-attacks – which are not to be confused with hacker attacks in everyday language or with armed attacks under *jus ad bellum* – are cyber operations causing injury or death to persons and damage to or destruction of objects.[52] The International Group of Experts drafting the Tallinn Manual pointed out that the act of violence referred to in Additional Protocol I does not apply only in a kinetic sense – it is sufficient to refer here to attacks conducted by chemical or biological weapons – but rather the decisive factor of identifying an operation as an 'attack' is the damage it caused.[53] Regarding electronic data, there was an understanding among experts that operations against data could only qualify as an attack if they were likely to cause results as described above (e.g. injury, death, etc.) or damage the

Review Of Red Cross Vol. 102, No. 1 (April 2020): 287, 328–329, 333 // DOI: doi.org/10.1017/S1816383120000387

43 Tim McCormack, "International Humanitarian Law and the Targeting of Data," *International Law Studies* 94 (2018): 222, 240; Kubo Mačák, *supra* note 6, 11.

44 Noam Lubell, "Lawful Targets in Cyber Operations: What the Principle of distinction Apply?" *International Law Studies* 89 (2013): 252, 268.

45 Kubo Mačák, "Military Objective 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israeli Law Review* Vol. 48, No. 1 (January 2015): 55, 67–77 // DOI: doi.org/10.1017/S0021223714000260

46 Heather A. Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," *Israel Law Review* Vol. 48, No. 1 (January 2015): 39, 41 // DOI:10.1017/S0021223714000272

47 *Ibid.,* 42.

48 ICRC, *Protecting Civilians against Digital Threats during Armed Conflict. Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations* (Geneva: International Committee of the Red Cross, 2023), 20.

49 *Ibid.,* 19.

50 Additional Protocol I, *supra* note 24, art. 49, para 1.

51 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, *supra* note 27, 603.

52 Michael N. Schmitt, *supra* note 14, 415.

53 *Ibid.,* 415.

functionality of a physical object. According to the experts, in this case the target is the person or material object affected by the operation.[54]

The majority of the experts involved in the private codification effort argued that damage to the functionality described above would only be considered an attack if it required the replacement of a physical component. On the other hand, for some experts remaining in the minority, deletion or manipulation of such data also qualifies as attack, as it will require the re-installation of software or the re-acquisition of the original data.[55] Others took a position in the process that it is immaterial how a material object loses functionality, but if it does, we are dealing with an attack.[56] Experts also agree that not all cyber operations can be considered as attacks, such as cyber espionage or actions that only cause inconvenience to the civilian population.[57]

It is clear that commentators are also divided as to whether operations against data can be characterized as an attack, since if one accepts the object status of electronic data, virtually every operation that causes damage (e.g. deletion, modification) to data will be considered an attack. However, the possibility of attacking data is not entirely excluded by those who do not agree with the former view. These authors were divided in terms of categorizing an attack on the functionality of physical objects. By way of example, according to Marco Roscini, cyber operations that are based on the deletion or alteration of data cannot be considered as attacks, but when carried out for military purposes, they should be regarded as military operations.[58] The author also points out that the Tallinn Manual's position on the restoration of functionality is doubtful, since the attacker cannot know in advance the form in which the damage caused will be remedied.[59] In his view, it is also unfortunate that, on the basis of the above interpretation, the shutting down of a State's banking system as a whole would not constitute an attack, but the destruction of a single server would.[60] Karine Bannelier argues that physical damage is not mandatory for an attack, as even the neutralization of military objectives may constitute an attack,[61] and Cordula Droege claims that even temporary loss of functionality is sufficient to find an attack.[62] On the other hand, according to Terry D. Gill, operations against registration of vital statistics, for instance birth or death, or against property records do not constitute an attack.[63]

It is generally accepted that operations affecting the availability of data do not constitute an attack, save for a very limited number of cases based on the consequences of the operation.[64] For example, according to Christopher S. Yoo, an attack with distributed denial of service (DDoS) would not qualify as an attack under IHL. Cyber espionage that undermines the confidentiality of data, such as a surveillance program, should also not be considered an attack.[65] Moreover, the collection of information

---

54 *Ibid.,* 416.
55 *Ibid.,* 417–418.
56 *Ibid.,* 418.
57 *Ibid*.
58 Marco Roscini, *supra* note 27, 178–189.
59 *Ibid.,* 180.
60 *Ibid*.
61 Karine Bannelier, "Is the principle of differentiation still relevant in cyberwarfare? From doctrinal discource to State's practice": 441; in: Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2021); Additional Protocol I, *supra* note 24, art. 52, para 2.
62 Cordula Droege, "Get off my cloud: cyber warfare, humanitarian law, and the protection of civilians," *International Review of the Red Cross* Vol. 94, No. 2 (June 2013): 533, 559 // DOI: doi.org/10.1017/S1816383113000246.
63 Terry D. Gill, *supra* note 35, 467.
64 Robin Geiß and Henning Lahmann, *supra* note 2, 567.
65 Christopher S. Yoo, *supra* note 34, 186.

cannot be regarded as illegal under the rules of IHL, although States have generally criminalized espionage in their domestic law.[66]

Consequently, the IHL assessment of counter-data operations depends heavily on the legal status of electronic data but operates partly within a broader framework. Furthermore, the significance of qualifying an operation as an attack lies in the fact that these are subject to the fundamental principles of IHL, such as distinction and proportionality.[67]

2. STATE PRACTICE

By its very nature, a scientific work on a question of international law cannot be complete without a careful analysis of State practice. This is important for two reasons. On the one hand*, ex post* practice in the application of a treaty is relevant to their interpretation. Indeed, the 1969 Vienna Convention on the Law of Treaties states that "[t]he treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms in their context and in the light of its object and purpose."[68] The Vienna Convention further provides that subsequent practice of the States Parties in the application of the treaty – which is the agreement of the States' Parties – should also be taken into account together with the context of the treaty for proper interpretation.[69] This also allows for an interpretation by the States' Parties of the provisions of Additional Protocol I which may differ from the original meaning from 1977. Subsequent practice however has its own limitations, since authentic interpretation can only result from the subsequent practice of all States' Parties in a relevant international treaty.[70]

On the other hand, State practice can also be seen as a constitutive element of customary international law, which is another source of international law in addition to international treaties, as stated by the International Court of Justice in the North Sea Continental Shelf case.[71] This source of international law also lays down binding standards for States, not parties, to Additional Protocol I, *e.g.* the United States and Israel to mention only a few major military powers, which are often almost identical to the treaty rules in this case.[72]

In order to analyze the subsequent practice of States Parties – admittedly as non-authentic interpretation – and State practice in general, it is essential to determine from where the change is measured. An excellent example for the necessity of this clarification is the assessment of the right to self-defense under the *jus ad bellum* regime, since a different starting point may lead to a drastically different outcome based on the same analytical criteria and methods.[73] In this specific situation, it was possible to conclude on the basis of Additional Protocol I and its commentary that, at the time of the adoption of the treaty and the status of customary law at the time, objects were

---

66 Amir Čengić, "Spies": 656; in: Dražan Dukić and Niccolò Pons, eds., *The Companion to International Humanitarian Law* (Leiden and Boston: Brill-Nijhoff, 2018).

67 *Ibid.,* 185; On these issues, see Karine Bannelier, *supra* note 60, 427–456; Terry D. Gill, *supra* note 35, 457–470.

68 *Vienna Convention on the Law of Treaties* (adopted 23 May 1969, entered into force 27 January 1980), 115 UNTS 331, art. 31 para 1.

69 *Ibid.,* art. 31, para 3(b).

70 Ori Pomson, *supra* note 39, 12.

71 *North Sea Continental Shelf,* Judgment, I.C.J. Reports 1969, p. 3, para 77. Another requirement for the development of customary law is the *opinio juris sive necessitatis*.

72 See for example Jean-Marie Henckaerts and Louise Doswald-Beck, *supra* note 26, rule 8–9.

73 Bence Kis Kelemen, *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására (Targeted Killing in International Law with special attention to the use of unmanned aerial vehicles)* (Pécs: Publikon, 2023), 102, 246.

understood to mean tangible, visible things, which did not include electronic data,[74] and consequently electronically stored personal data. Therefore, the article examines below the change in the interpretation of the treaty in question, and customary international law from this point of departure.

When analyzing State practice, each State's position can be divided into one of five categories: electronic data is an object (1), electronic data is not an object (2), ambiguous (3), States, that expressed views on international law applicable in cyberspace, but did not comment on the issue at hand and (4) States which have not made a statement nor expressed their position in a way, which manifested in academic work (5).

For example, in its 2020 statement, Israel *expressis verbis* excluded computer data from the category of objects, referring to the fact that only tangible things can be considered as such under current international law.[75] Similarly, Denmark categorically rejects the object status of digital data.[76] Although not so clearly, New Zealand also tends to oppose to the object status of data by taking the view that only cyber operations that cause physical damage could be perceived as an attack.[77] Since under IHL solely military objectives can be attacked, physical damage can only occur in the case of attacking a physical object or person. Chile assert that data in general are not objects, due to their non-visible, non-tangible nature; however it also claims that States should not attack data, if that would affect the civilian population, save for situations, in which the data in question were used for military purposes.[78] The United Kingdom regards all operations as attacks which have the same or similar effects as a kinetic measure,[79] so that attacks on electronic data as objects are not relevant to the State in this respect. Australia took the same position.[80]

In comparison, already in 2019 France determined that modifications, deletions, and operations against the availability of digital data would be considered an attack, thereby indirectly recognizing these data as objects.[81] In particular, France has pointed out *expresses verbis* as well, that data may be protected objects under IHL, and a contrary view would be hard to reconcile with the object and purpose of the law of armed conflict in the current digital world.[82] There is, however, some contradiction in

---

74 See Part 2.

75 Roy Schöndorf, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations* (December 2022) // https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

76 *Military Manual on International Law Relevant to the Danish Armed Forces in International Operations* (Denmark: Danish Ministry of Defence – Defence Command Denmark, 2016), 292. This is further reinforced in Denmark's position paper in 2023, *expressis verbis* dealing with this issue. See Jeppe Mejer Kjelgaard and Ulf Melgaard "Denmark's Position Paper on the Application of International Law in Cyberspace," *Nordic Journal of International Law* Vol. 94, No. 3, 9–10 // DOI: https://doi.org/10.1163/15718107-20230001

77 New Zealand Foreign Affairs & Trade, *The Application of International Law to State Activity in Cyberspace* (2020): para 25 // https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

78 *Report of the Inter-American Juridical Committee. Second Report: International Law Applicable to Cyberspace*, CJI/doc. 671/22, rev. 2, corr. 1 (October 2022), 19.

79 Government of United Kingdom, Foreign Commonwealth & Development Office, *Policy Paper. Application of international law to states' conduct in cyberspace: UK statement* (2021): para 24 // 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#international-humanitarian-law-ihl.

80 Australian Government, *Annex B: Australia's position on how international law applies to State conduct in cyberspace* (2020): point 2 // https://www.internationalcybertech.gov.au/our-work/annexes/annex-b

81 Ministrè re des Armées, *Droit International appliqué aux Opérations dans le Cyberspace* (2019): 13–14, 18 // https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf

82 *Ibid.,* note 79.

the French position, since DDoS-type actions and the collection of information were not regarded as an attack, although DDoS operations temporarily make it impossible to access certain data, which in turn falls within the concept of attack defined at the end of the French statement, i.e. an operation against the availability of data.[83] Similarly, Germany considers actions that generate adverse effects against information as an attack.[84] Romania took the view that IHL was applicable to cyber operations and data can only be attacked when it is considered to be a military objective, and by definition an object.[85] Finland – using an interesting approach – also *expressis verbis* recognizes the object status of digital data, in particular civilian data as civilian objects.[86] Norway also asserts, that electronic data are objects.[87] Recently Costa Rica also endorsed the view of incorporating civilian data into the notion of civilian objects.[88] Ireland in 2023 asserted that the notion attack would cover cases of loss of functionality to networks or electronic systems.[89] This means that operations against data should be seen as attacks, in other words data should be an object for Ireland. This conclusion is further reinforced in the reference in Ireland's Position Paper to the ICRC's own Position paper outlining the civilian data are civilian objects idea.[90] Last, but not least, Pakistan also seems to subscribe to the view that civilian objects also encompass civilian data.[91]

In addition, a significant number of States have taken an ambiguous position on the issue. For example, Italy stated in 2021 that attacks on critical infrastructure, in so far as they affect functionality, are considered attacks.[92] This could potentially mean that electronic data are objects due to the deletion of operational-level data in critical infrastructures, but it can also mean that the replacement of a physical component is necessary to restore functionality. Switzerland expressed that categorizing data is a challenge, while noting that a responsible actor should be able to assess the potential

---

83 *Ibid.,* 13, cf. 18.

84 The Federal Government of Germany, *On the Application of International Law in Cyberspace. Position Paper* (March 2021): 8 // https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

85 UNGA, *Official compendium of voluntary national contributions on the subject of how international law apply to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly 73/266* (13 July 2021), A/76/136*, 8. (hereinafter: A/76/136*).

86 *International law and cyberspace. Finland's national positions* (2020): 7 // https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

87 This also translates to the conclusion, that cyber operations causing loss of functionality where merely reinstallation is required are also attacks in the understanding of Norway. See *Manual of the Law of Armed Conflict* (Norway: The Chief of Defence, 2013), 210.

88 Costa Rica further explains, that previously data such as medical, social security, tax, *etc.* were stored on paper files protected under IHL, which also warrants for their protection now, when they are stored electronically. Please do mind that almost all type of data mentioned by Costa Rica are also personal data. See *Costa Rica' Position on the Application of International Law in Cyberpsace* (2021): 13–14 // https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf

89 Ireland Department of Foreign Affairs, *Position Paper on the Application of International Law in Cyberspace* (2023): para 31 // https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf.

90 *Ibid., supra* note 22.

91 It needs to be noted in case of Pakistan, that the State's views are not entirely compatible with the mainstream understanding of international law. For instance, Pakistan calls for outlawing (under IHL) not only deleting, destroying or manipulation essential data for critical civilian infrastructure, but also information operations and perhaps cyberespionage as well. See *Pakistan's Position on the Application of International Law in Cyberspace* (March 2023): para 14 // https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf

92 *Italian Position Paper on 'International Law and Cyberspace* (2021): 9–10 // https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

impact of its conduct and any resulting harm.[93] Opting for a very similar approach, Brazil claims that, while IHL applies to cyberspace, the question whether civilian data should be considered civilian object as well deserves further attention.[94] The legal position of the United States should also be classified as ambiguous despite the fact that in 2016, some data were clearly identified as a military objectives.[95] However, in 2021, this was no longer included in its position paper; but neither is it possible to conclude to the contrary.[96]

The ICRC held a regional consultation on issues of the application of IHL in cyberspace among various States and some of the results of these exchange of ideas have already been published. No specific individual position was adopted by the States participating in these workshops, however important conclusions can be drawn from the ideas exchanged. For example, Latin American States were invited on a consultation from 9 to 11 November 2021. The ICRC report of the workshop shows that participants were also uncertain as to the object status of civilian data. While the participating States agreed that this concept should be interpreted in light of changing circumstances, and that electronic data are regarded as an 'object' in several Latin American national legal systems, no clear position was taken.[97] A similar position has been made by several Central and Eastern European States as well in another regional consultation on 8 December 2021. The participants acting in their personal capacity agree that an evolutionary interpretation of IHL is warranted in case of data, since not qualifying them as objects would go counter to the object and purpose of IHL and create a protection gap. Furthermore, such a qualification would also be more practical from a military perspective. Conversely, the participating States were keen not to take a straightforward position.[98] Although this would make it possible to categorize participating States as supporters of the object status of digital data, the moderator of the panels dealing with the issue was Kubo Mačák,[99] who is an open supporter of the 'electronic data are objects' position. This may have influenced the position of the experts of the participating States, which warrants for caution when interpreting these positions.

Many States, while expressing their position regarding the norms of international law applicable to cyberspace, did not articulate their views on the legal nature of computer data. For example, in its 2022 statement, Canada defined attacks on the basis of a traditional interpretation of the Tallinn Manual, but did not comment on the object status of the data.[100] Japan has taken a similar position, omitting to assess the legal nature of electronic data.[101]

---

93 Federal Department of Foreign Affairs, *Switzerland's position paper on the application of international law in cyberspace* (2021): 10 // https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf

94 A/76/136* 23.

95 Brian J. Egan, *International Law and Stability in Cyberspace, Berkeley Law, 10 November 2016* (November 2016): 9 // https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

96 A/76/136*, *supra* note 84, 136–142.

97 Kubo Mačák, *Regional Consultation of Latin American States, 9–10 November 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts* (Geneva: International Committee of the Red Cross, 2022), 8.

98 Tatiana Jančárková and Kubo Mačák, *Regional Consultation of Central and Eastern European States, 8 December 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts* (Geneva: International Committee of the Red Cross, 2022), 7.

99 Kubo Mačák, *supra* note 96, 7; *Ibid.,* 7.

100 Government of Canada, *International Law applicable in cyberspace* (2022): para 49 // https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a14

101 Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (2021): 7 // https://www.mofa.go.jp/files/100200935.pdf

The distribution of State practice is demonstrated in the table below:

Table 1. State practice on the interpretation of electronic data[102]

Electronic data is an object	Electronic data is NOT an object
Norway (2013), France (2019), Finland (2020), Germany (2021), Romania (2021), Costa Rica (2023), Ireland (2023) Pakistan (2023)	Denmark (2016, 2023), Israel (2020), New Zealand (2020), Australia (2020), United Kingdom (2021)
Ambiguous	Not taking a position, but commented on international law applicable in cyberspace
Italy (2021), Switzerland (2021), United States (2016, 2021), Brazil (2021), Argentina (2021), Bolivia (2021), Colombia (2021), Ecuador (2021), Mexico (2021), Nicaragua (2021), Paraguay (2021), Peru (2021), Uruguay (2021), Sweden (2022), Czech Republic (2022), Estonia (2022), Hungary (2022), Latvia (2022), Lithuania (2022), Poland (2022), Slovenia (2022)	The Netherlands (2019), Iran (2020), Kenya (2021), Japan (2021), Singapore (2021), China (2021), Russia (2021), Kazakhstan (2021), Canada (2022), Sweden (2022)

Although the analysis of State practice is concluded here, it is important to mention the position of an indispensable actor for the application of IHL, which is the ICRC. In its position paper, the organization highlighted that the deletion or modification of civilian data, including personal data such as social security, taxation or banking data, is capable of causing more damage than the destruction of a physical object.[103] On that basis, according to the ICRC, the categorization of computer data as a non-object runs counter to the object and purpose of IHL.[104]

CONCLUSIONS

Several conclusions can be drawn from the analysis above. First, at the time when military objectives and civilian objects were defined, electronic data was virtually of no concern.[105] Consequently, Additional Protocol I followed that logic and that customary international law also developed accordingly.

Second, international law scholars are divided on whether computer data can be considered an object and thus civilian data, including personal data, could be targeted in military operations. In contrast, it seems generally accepted that certain data, which usually coincides with the category of personal data, (e.g. medical data) are subject to specific protections under IHL. However, the cited positions of commentators outline

[102] In addition to the above primary sources and the ICRC reports *supra* note 96 and *supra* note 97, the article relied on the International Cyber Law in Practice Interactive Toolkit. See National Positions: https://cyberlaw.ccdcoe.org/wiki/Category:National_position. Those States which did not offer a position on international law on cyberspace are not included in the table, but their high number is easily conceivable.

[103] 32IC/15/11, *supra* note 4, 43.

[104] "International humanitarian law and cyber operations during armed conflicts. 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. 1 (March 2021): 490 // DOI: doi.org/10.1017/S1816383120000478.

[105] This is true even if the Soviet Union talked about cyber attacks in the 1980's. See Ori Pomson, *supra* note 39, 20.

a trend whereby an increasing number of scholars regard electronic data as objects. Admittedly, there are convincing policy considerations behind protection civilian data as objects, which revolve around the fact, that certain civilian data (medical, social security, banking, tax etc.) significantly affect the life of the civilian population, consequently manipulating with or deleting such data – which are can also be considered personal data at the same time – could cause systematic problems for civilians.

Third, an assessment of State practice shows that States are also divided on the issue. In a sample of forty-four States examined, only eight took the view that computer data could be considered an object, while five expressly opposed such an interpretation. A considerable number of States, precisely twenty-one, were uncertain on the issue, and ten did not take a position despite expressing their views on cyberspace to some extent.

In light of the fact that both *ex post* practice in the application of a treaty and a change in customary international law would require at least a considerable degree of uniform State practice, and the practice of all States Parties would be required for the authentic interpretation of a treaty in through subsequent practice, it is not possible to establish a change from the interpretation of objects under IHL from its starting point in 1977. This means that electronic data, and thus personal data processed electronically, generally cannot be considered objects, and thus civilian data are not protected under IHL, save for the narrow exceptions of medical data, which are incorporated into physical medical facilities and data that is stored on paper.

However, State practice shows on the one hand that the international community has a large number of ambiguous States. This means two things: first, if the ambiguity would be resolved for the acceptance of data as objects, that would be a clear trend towards this position in the international community. Second, the geographical distribution of State practice indicates that if some uncertain States, for instance Latin American, Central and Eastern European countries, developed their positions in line with the principles laid down by the ICRC, this could also lead to the development of regional customary law, thus contributing to fragmentation of international law. On the other hand, State practice is also shows that the Tallinn Manual has a great influence on how States formulate their position on international law applicable in cyberspace, and reference can be made to the notion of attack in many position papers. Not only does the Tallinn process seem to have an effect, the ICRC Regional Consultation series also bore fruit as Costa Rica not only adopted a national position after the consultation but taken a similar view to the ICRC. Poland also published a national position in 2022 after the regional consultation for Central and Eastern European States have ended.

A brief comparison of the data protection regimes of the IHL and the GDPR is necessary for determining whether GDPR or any similar data protection laws have anything to offer when it comes to developing IHL. Article 5(1) and (2) of the GDPR set out the basic principles of the processing of personal data such as lawfulness, fairness and transparency, purpose limitation, accuracy, storage limitations, integrity and confidentiality, and accountability. First, most of these principles are, by their very nature, inapplicable in an armed conflict scenario – these are lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation and accuracy. The principle of confidentiality, i.e. protection against unauthorized or unlawful processing, is generally disregarded as a norm of IHL, since cyber espionage is legal under international law. The only contrary practice that could be found is that of Pakistan, and an ambiguous partial statement from France referenced above.

This article is centered around the principle of integrity – in other words, protection against deletion, modification, or alteration of data. As was established, this principle has not yet crystallized in the framework of IHL, but it cannot be fully disregarded, as scholarly support for this principle is growing and ever more States seem to back up this position.

As a *lex ferenda,* it would be an interesting thought experiment whether the above-mentioned data protection principles, enshrined in the GDPR, would be applied in armed conflicts. However, this article suggests that the inclusion of these principles would not further the protection of the civilian population during hostilities.

Military operations are data-intensive endeavors. For example, a targeted killing operation, which could be defined as lethal use of force with the intent, deliberation and premeditation to kill individually selected persons,[106] requires a tremendous amount of data in order to be lawful. Within the context of an armed conflict a targeted killing operation among others must adhere to the principles of military necessity, distinction, proportionality, humanity, and precautions.[107] For our purposes, the most relevant principle will be distinction, which requires that parties of the conflict distinguish between the civilian population and combatants/persons directly participating in hostilities as well as civilian objects and military objectives.[108] In non-international armed conflicts, the determination whether a person is directly participating in hostilities or assuming a continuous combat function[109] presupposes a vast amount of data, including personal data collected, processed, and interpreted on the lives of these individuals.

By implementing other principles of data protection, for instance data minimization or storage limitation, collection of data necessary for the determination of targetability would become increasingly difficult or even impossible. Although Additional Protocol I prescribes that, in case of doubt, parties should consider a person civilian for the purpose of targetability,[110] this would open the door for arbitrary determinations of a person's status under IHL based on insufficient information.

It is therefore in the interest of the civilian population not to incorporate unnecessary data protection principles into the delicate balance of targeting that IHL provides, since it could significantly increase the threat of contrafactual determination of targetability in a number of scenarios. Consequently, the general protective functions of IHL should prevail over the fundamental rights principles of data protection in times of armed conflict.

BIBLIOGRAPHY

1. *Costa Rica' Position on the Application of International Law in Cyberpsace*. (2021) // https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf

[106] Nils Melzer, *Targeted Killing in International Law* (New York: Oxford University Press, 2008), 5.
[107] Nils Melzer, *International Humanitarian Law. A Comprehensive Introduction* (Geneva: International Committee of the Red Cross, 2016), 17–20.
[108] Additional Protocol I, *supra* note 24, art. 48, art. 51 para. 3.
[109] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, (Geneva: International Committee of the Red Cross, 2009), 27, 34.
[110] Additional Protocol I, *supra* note 24, art. 50 para. 1.

2. "International humanitarian law and cyber operations during armed conflicts. 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. 1 (March 2021): 481–492. // DOI: doi.org/10.1017/S1816383120000478
3. *International law and cyberspace. Finland's national positions.* (2020) // https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727
4. *Italian Position Paper on 'International Law and Cyberspace'.* (2021) // https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf
5. *Manual of the Law of Armed Conflict*. Norway: The Chief of Defence, 2013.
6. *Military Manual on International Law Relevant to the Danish Armed Forces in International Operations*. Denmark: Danish Ministry of Defence – Defence Command Denmark, 2016.
7. *Pakistan's Position on the Application of International Law in Cyberspace*. (March 2023) // https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf
8. *Report of the Inter-American Juridical Committee. Second Report: International Law Applicable to Cyberspace*. CJI/doc. 671/22, rev. 2, corr. 1 (October 2022).
9. Akende, Dapo, Coco, Antonio and de Souza Dias, Talita. "Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies." *International Law Studies* 99 (2022): 5–25.
10. Australian Government. *Annex B: Australia's position on how international law applies to State conduct in cyberspace.* (2020) // https://www.internationalcybertech.gov.au/our-work/annexes/annex-b
11. Bannelier, Karine. "Is the principle of differentiation still relevant in cyberwarfare? From doctrinal discource to State's practice": 426–455. In: Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing, 2021.
12. Benvenisti, Eyal. "The Birth and Life of the Definition of Military Objectives." *International & Comparative Law Quarterly* Vol. 71, No. 2 (May 2022): 269–295 // DOI:10.1017/S0020589322000100
13. Boothby, William H. "Cyber Capabilities": 85–136. In: William H. Boothby, ed., *New Technologies and the Law in War and Peace.* Cambridge: Cambridge University Press, 2019.
14. Čengić, Amir. "Spies": 656–658. In: Dražan Dukić and Niccolò Pons, eds., *The Companion to International Humanitarian Law.* Leiden and Boston: Brill-Nijhoff, 2018.
15. Droege, Cordula. "Get off my cloud: cyber warfare, humanitarian law, and the protection of civilians." *International Review of the Red Cross* Vol. 94, No. 2 (June 2013): 533–578. // DOI:10.1017/S1816383113000246
16. Ega, Brian J. *International Law and Stability in Cyberspace, Berkeley Law, 10 November 2016.* (November 2016) // https://www.justsecurity.org/wp-content/

uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

17. Federal Department of Foreign Affairs. *Switzerland's position paper on the application of international law in cyberspace.* (2021) // https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf
18. Geiß, Robin, and Lahmann, Henning. "Protection of Data in Armed Conflict." *International Law Studies* 97 (2021): 557–572.
19. Gill, Terry D. "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict": 456–469. In: Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing, 2021.
20. Gisel, Laurent, Rodenhäuser, Tilman and Dörmann, Knut. "Twenty years on: International humanitarian law and the protection of civilians against effects of cyber operations during armed conflicts." *International Review Of Red Cross* Vol. 102, No. 1 (April 2020): 287–334 // DOI:10.1017/S1816383120000387
21. Government of Canada. *International Law applicable in cyberspace*. (2022) // https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a14
22. Government of United Kingdom, Foreign Commonwealth & Development Office. *Policy Paper. Application of international law to states' conduct in cyberspace: UK statement*. (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#international-humanitarian-law-ihl
23. Harrison Dinniss, Heather A. "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives." *Israel Law Review* Vol. 48, No. 1 (January 2015): 39–54 // DOI: doi.org/10.1017/S0021223714000272
24. Henckaerts, Jean-Marie and Doswald-Beck, Louise. *Customary International Humanitarian Law – Volume I: Rules.* New York: International Committee of the Red Cross – Cambridge University Press, 2005.
25. ICRC. *International humanitarian law and the challenges of contemporary armed conflicts report*. Geneva: International Committee of the Red Cross, 2015, 32IC/15/11.
26. ICRC. *Protecting Civilians against Digital Threats during Armed Conflict. Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations.* Geneva: International Committee of the Red Cross, 2023.
27. Ireland Department of Foreign Affairs. *Position Paper on the Application of International Law in Cyberspace.* (2023) // https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf
28. Jančárková, Tatiana and Mačák, Kubo. *Regional Consultation of Central and Eastern European States, 8 December 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts.* Geneva: International Committee of the Red Cross, 2022.

29. Mejer Kjelgaard Jeppe and Melgaard, Ulf. "Denmark's Position Paper on the Application of International Law in Cyberspace." *Nordic Journal of International Law* Vol. 94, No. 3, 9–10 // DOI: https://doi.org/10.1163/15718107-20230001
30. Kis Kelemen, Bence. *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására* (*Targeted Killing in International Law with special attention to the use of unmanned aerial vehicles).* Pécs: Publikon, 2023.
31. Kittichaisaree*,* Kriangsak. *Public International Law of Cyberspace.* Cham: Springer, 2017.
32. Lubell, Noam. "Lawful Targets in Cyber Operations: What the Principle of distinction Apply?" *International Law Studies* 89 (2013): 250–275.
33. Lumiste, Liina. "Russian Approaches to Regulation Use of Force in Cyberspace." *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 109–132 // DOI: doi.org/10.1163/22115897_02001_007
34. Mačák, Kubo. "Military Objective 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." *Israeli Law Review* Vol. 48, No. 1 (January 2015): 55–80 // DOI: doi.org/10.1017/S0021223714000260
35. Mačák, Kubo. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." *Israel Law Review* Vol. 48, No. 1 (January 2015): 55–80 // DOI: doi.org/10.1017/S0021223714000260
36. Macák, Kubo. "This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace." *Exeter Centre for International Law Working Paper Series* 2/2019 (2019): 1–17.
37. Mačák, Kubo. "Regional Consultation of Latin American States, 9–10 November 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts." Geneva: International Committee of the Red Cross, 2022.
38. McCormack, Tim. "International Humanitarian Law and the Targeting of Data." *International Law Studies* 94 (2018): 220–240.
39. Melzer, Nils. *International Humanitarian Law. A Comprehensive Introduction.* Geneva: International Committee of the Red Cross, 2016.
40. Melzer, Nils. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.* Geneva: International Committee of the Red Cross, 2009.
41. Melzer, Nils. *Targeted Killing in International Law.* New York: Oxford University Press, 2008.
42. Mimran, Tal. "Between Israel and Iran: Middle-East Attitudes to the Role of International Law in the Cyber-Sphere." *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 209–235 // DOI: doi.org/10.1163/22115897_02001_011
43. Ministrè re des Armées. *Droit International appliqué aux Opérations dans le Cyberspace.* (2019) // https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf
44. Ministry of Foreign Affairs of Japan. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* (2021) // https://www.mofa.go.jp/files/100200935.pdf
45. New Zealand Foreign Affairs & Trade. *The Application of International Law to State Activity in Cyberspace.* (2020) // https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

46. Pomson, Ori. "'Objects'? The Legal Status of Computer Data under International Humanitarian Law." *Journal of Conflict & Security Law* Vol. 28, No. 2 (January 2023): 349–387 // DOI:doi.org/10.1093/jcsl/krad002
47. Representaciones Diplomáticas de Cuba en El Exterior. *71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*. (June 2017) // https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information
48. Roscini, Marco. *Cyber Operations and the Use of Force in International Law.* Cambridge: Cambridge University Press, 2014.
49. Sandoz, Yves, Swinarski, Christophe and Zimmermann. Bruno. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.* Geneva: International Committee of the Red Cross, 1987.
50. Schmitt, Michael N. "International cyber norms: reflections on the path ahead." *Netherlands Military Law Review* 111 (2018): 1–12.
51. Schmitt, Michael N. "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision." *Israel Law Review* Vol. 48, No. 1 (March 2015): 81–109 // DOI:10.1017/S0021223714000314
52. Schmitt, Michael N. "Wired warfare 3.0: Protecting the civilian population during cyber operations." *International Review of Red Cross* Vol. 101, No. 1 (April 2019): 333–355 // DOI:10.1017/S1816383119000018
53. Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017.
54. Schöndorf, Roy. *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*. (December 2022) // https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/
55. Shany, Yuval and Mimran, Tal. "International Regulation of Cyber Operations." *Hebrew University of Jerusalem Legal Studies Research Paper Series* 5/2021, (November 2021): 1–24.
56. The Federal Government of Germany. *On the Application of International Law in Cyberspace. Position Paper.* (March 2021) // https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf
57. UNGA. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. (24 June 2013), UN Doc A/68/98.
58. UNGA. *Official compendium of voluntary national contributions on the subject of how international law apply to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly 73/266.* (13 July 2021), A/76/136*.
59. Watt, Eliza. *State Sponsored Cyber Surveillance. The Right to Privacy of Communications and International Law.* London: Edward Elgar, 2021.
60. Yoo, Christopher S. "Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures": 175–194. In: Jens David Ohlin, Kevin

Govern and Claire Finkelstein, eds., *Cyberwar. Law and Ethics for Virtual Conflicts.* Oxford: Oxford University Press, 2015.

61. Zhu, Lixin and Chen, Wei. "Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Coexistance." *Baltic Yearbook of International Law Online* Vol. 20, No. 1 (December 2022): 187–208 // DOI: doi.org/10.1163/22115897_02001_010

LEGAL REFERENCES

1. *Charter of Fundamental Rights of the European Union* (adopted 7 December 2000, entered into force 1 December 2009), OJ C 326.
2. *Convention for the Protection of Human Rights and Fundamental Freedoms* (adopted 4 November 1950, entered into force 3 September 1953), ETS 005.
3. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (adopted 28 January 1981, entered into force 1 October 1985), ETS 108.
4. *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976), 999 UNTS 171 (ICCPR).
5. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion, I.C.J. Reports 1996*,* p. 226.
6. *North Sea Continental Shelf.* Judgement, I.C.J. Reports 1969, p. 3.
7. *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I)* (adopted 8 June 1977, entered into force 7 December 1979), UNTS 1125 3.
8. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Official Journal, 2016, no. L 119.
9. *Vienna Convention on the Law of Treaties* (adopted 23 May 1969, entered into force 27 January 1980), 115 UNTS 331.