ON THIN ICE: QUALIFICATION OF CYBER-ATTACKS ON PERSONAL DATA UNDER INTERNATIONAL HUMANITARIAN LAW

ABRASHIN R.

Roman Abrashin — Junior Associate, Center of International Law at Chistye Prudy, Moscow, Russia (rpabrashin@gmail.com).
ORCID: 0000-0003-4891-359X.

Abstract

The article examines the possibility and conditions for qualifying cyber-attacks on personal data as a military operation, an attack, and/or an armed conflict from the perspective of international humanitarian law (hereinafter — IHL). It is often personal data that is the target of a cyber-attack. In this context, potential legal qualification of a cyber-attack depends on whether and to what extent states recognise data as an "object" under IHL. In the absence of a specific treaty dealing with the application of IHL to the malicious use of information and communication technologies (hereinafter — ICTs), the main focus of the study is on the existing sources of IHL (Geneva Conventions, Additional Protocols, principles), customary international law as well as judicial decisions and legal teachings as subsidiary means for the determination of rules of law. Special attention is paid to the positions of the Russian Federation and the United States on the issue of the application of IHL to cybernetic activities. The author concludes that a cyber-attack on personal data can qualify as a military operation, an attack and a prerequisite for the outbreak of an armed conflict, and offers possible qualification criteria. At the same time, "stretching" *jus in bello* to the activities involving ICTs creates threats for the international community due to prospective militarisation of "cyberspace".

Key words

cyber-attack, *jus in bello*, attack, armed conflict, personal data

Citation: Abrashin R. *On Thin Ice: Qualification of Cyber-Attacks on Personal Data under International Humanitarian Law* // Zhurnal VSHÉ po mezhdunarodnomu pravu (HSE University Journal of International law). 2024. Vol. 2. № 4. P. 36–52.

https://doi.org/10.17323/jil.2024.24743

Introduction

Wars between states have been waged for many centuries. With the development of mankind and political entities, the means and methods of warfare have been improved. There has been a rapid evolution from a wooden bow with arrows to nuclear weapons. In the *Nuclear Weapons Advisory Opinion,* the International Court of Justice (hereinafter — ICJ) reaffirmed the application of the principles of IHL both to all forms of warfare and to all kinds of weapons past, present and future.[1] In the XXI century, the militarisation has affected the advanced ICTs. As a result, "cyberspace" is becoming a new domain of hostilities where states are accustomed to launching cyber operations or cyber-attacks against their adversaries.[2] Thus, in the mid-2000s, the perspective of some armed conflicts changed to a new platform for conducting military operations. The question is, whether cyber-attacks can be qualified as a military operation or an attack, or serve as a precondition for the outbreak of hostilities.

The subject-matter of the present study is relatively novel within the Russian doctrine of public international law. Prior to this paper, the concept of "cyberspace" and the application of international law to it were addressed in writings by a number of legal scholars.[3] However, only some experts raised the question of the application of IHL norms to "cyberspace".[4] For example, S. Garkusha-Bozhko analyzed

1 ICJ. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion of 8 July 1996. § 86.

2 Schmitt M. N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge : Cambridge University Press, 2013 (hereinafter — Tallinn Manual). P. 10.

3 See e.g., Rusinova V. N. *Mezhdunarodno-pravovoy printsip nevmeshatel'stva i kiberoperatsii: neopravdannye ozhidaniya?* [*The International Legal Principle of Non-Interference and Cyber-Operations: Unjustified Expectations?*] // Mezhdunarodnoe pravosudie. 2018. Vol. 25. № 1. P. 38–52; Rusinova V. N. *Mezhdunarodno-pravovaya kvalifikatsiya vredonosnogo ispol'zovaniya informatsionno-kommunikatsionnaykh technologii: v poiskakh konsesusa* [*Qualification of Harmful Use of Information and Communications Technologies Under International Law: In Search of a Consensus*] // Moscow Journal of International Law. 2022. № 1. P. 38–51; Ivanova K. A., Myltykbaev M. Zh., Shtodina D. D. *Ponyatie kiberprostranstva v mezhdunarodnom prave* [*The Concept of Cyberspace in International Law*] // Pravoprimenenie. 2022. Vol. 6. № 4. P. 32–44; Kapustin A. Ya. *Suverenitet gosudarstva v kiberprostranstve: mezhdunarodno-pravovoe izmerenie* [*State Sovereignty in Cyberspace: International Legal Dimension*] // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'noogo pravovedeniya. 2022. Vol. 18. № 6. P. 99–108.

4 See e.g., Manevich V. V. Mezhdunarodno-pravovoe regulirovanie primeneniya kibersredstv pri vedenii vooruzhennykh konfliktov: pravovye osnovy i nauchnye discussii [*International Legal Regulation of the Use of Cyber Means in Armed Conflicts:*

the qualification of a cyber-attack as an “attack” within the meaning of Article 49 of Additional Protocol I (hereinafter — AP I) of 8 June 1977 to the Geneva Conventions of 12 August 1949, which relates to the protection of victims of international armed conflicts.[5] In another article, he attempted to define the concept of armed conflict in “cyberspace”.[6] V. Rusinova in her research also drew attention to the misuse of the *military paradigm* by some states, leading to a blurring of the boundaries between military and non-military use of ICTs.[7] The issues of the application of IHL to “cyberspace” have been more extensively researched in the foreign academic literature.[8] That said, while there have been previous attempts to qualify cyber-attacks on critical infrastructure, the present paper focuses on personal data which is highly vulnerable to cyber-attacks.[9] Thus, the novelty of this study is that it attempts to qualify cyber-attacks on personal data under IHL using the method of evolutionary interpretation of the concepts of military operation, attack, and armed conflict.

The research question of the study is whether and under what conditions cyber-attacks can be qualified as a military operation, an attack, or an armed conflict. This qualification relates, in particular, to the recognition of data as an “object” under IHL. Thus, the legal qualification of cyber-attacks depends on whether and to what extent states recognise data as an “object” under IHL.

The methodology of the study is legal positivism. In this respect, the research is mainly based on treaty law (Geneva Conventions and Additional Protocols). Also, in the absence of a specific “cyber” treaty, the focus of the analysis is on state practice (official positions of states on the issue of the application of IHL to “cyberspace”) and *opinio juris*, both of which are constituent elements of international custom. In addition to treaty and customary law, judicial decisions are of paramount importance in interpreting the concepts of IHL. In this regard, the author focuses on the jurisprudence of the European Court of Human Rights (hereinafter — ECtHR), the ICJ, the International Criminal Court (hereinafter — ICC), and the International Tribunal for the Former Yugoslavia (hereinafter — ICTY). Although the International Committee of the Red Cross’s position paper and the Tallinn Manuals are not legally binding sources of international law, the author refers to them as “legal teachings” in the meaning of Article 38 of the Statute of the ICJ.[10] So judicial decisions and legal teachings are used as subsidiary means for the determination of rules of law. The main tool for analysing the concepts of military operation, attack and armed conflict in the cyber context will be an evolutionary method of interpretation.

The paper is structured as follows: an introduction, six sections, and concluding remarks. The first section discusses the terminology used to describe activities in “cyberspace”. The next part is dedicated to the analysis and interpretation of three key concepts, such as a military operation, an attack and an armed conflict. The third part addresses the classification of the official positions of states on the applicability of IHL to “cyberspace”. The fourth section covers theoretical approaches and official positions on the question of whether data should be considered an “object” under IHL. The fifth part of the study considers a range of potential scenarios in which cyber-attacks on personal data may be qualified as a military operation, an attack, and an armed conflict, and the final section compares the official positions of the Russian Federation and the United States.

Legal Foundations and Scientific Discussions] // Zakon i Pravo. 2024. Vol. 12. № 2. P. 275–282; Garkusha-Bozhko S.Yu. Opredelenie vooruzhennogo konflikta v kiberprostranstve [*The Definition of Armed Conflict in Cyberspace*] // Vestnik of Saint Petersburg University. Law. 2023. Vol. 14. № 1. P. 194–210; Garkusha-Bozhko S. Yu. *Mezhdunarodnoe gumanitarnoe pravo v kiberprostranstve: ratione materiae, ratione temporis i problema kvalifikatsii kiberatak* [*International Humanitarian Law in Cyberspace: Ratione Materiae, Ratione Temporis and Problem of Cyber-Attack Qualification*] // Tsifrovoe pravo. 2021. Vol. 2. P. 64–82.

5 Garkusha-Bozhko S. Yu. *Mezhdunarodnoe gumanitarnoe pravo v kiberprostranstve…* P. 80.

6 Garkusha-Bozhko S. Yu. *Opredelenie vooruzhennogo konflikta…* P. 207.

7 Rusinova V. N. *Mezhdunarodno-pravovaya kvalifikatsiya…* P. 47.

8 See e.g., Roscini M. *Cyber Operations and the Use of Force in International Law*. Oxford : Oxford University Press, 2014; Laurent G., Tilman R., Knut D. *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. 2022. Vol. 102. № 913. P. 287–334; Chang Z. *Cyberwarfare and International Humanitarian Law* // Creighton International and Comparative Law Journal. 2017. Vol. 9. № 1. P. 29–53; Veljković S. *Possibility of Applying the Rules of International Humanitarian Law to Cyber Warfare* // Pravo – Teorija I Praksa. 2024. Vol. 41. № 3. P. 17–28.

9 For example, DDoS attacks on personal data of civilians in the context of the Russian-Ukrainian conflict or cyber-attacks infiltrating databases and releasing their contents during the Israeli-Hamas conflict.

10 The Statute of the International Court of Justice (adopted on 26 June 1945, and entered into force on 24 October 1945).

1. “ICT” and “cyber” terminology

There are currently two terminological approaches to the definition of activities in “cyberspace”. In the documents adopted under the auspices of the United Nations the “ICT” terminology is employed.[11] The “cyber” terms are mostly used by the experts of the Tallinn Manuals[12] and the legal advisers of the ICRC,[13] as well as in cybersecurity strategies and national positions of certain Western states. The choice of terminology used depends on the state’s stance. There are three formulations found in the official positions of states: “use of ICTs”, “cyber operations”, and “cyber-attacks”. The first term “use of ICTs” is used, for example, by Kazakhstan,[14] Kenya[15] and the Russian Federation.[16] The term “cyber operations” is employed by the majority of states which have expressed a position on the application of international law in “cyberspace”, such as Pakistan,[17] Romania,[18] Singapore[19] and the United States.[20] The third term “cyber-attacks” is found in the official positions of Cuba,[21] the Czech Republic,[22] Germany,[23] and New Zealand.[24]

As mentioned earlier, cyber terminology is actively employed by the experts of the Tallinn Manuals and the ICRC’s legal advisers. Thus, in the November 2019 position paper, the ICRC’s legal advisers define cyber operations as “operations against a computer system or network or other connected device through a data stream, when used as means and methods of warfare in the context of an armed conflict”.[25] In another report, the ICRC’s legal advisers use the term “cyber warfare”.[26] In contrast, the recent resolution of the 34th International Conference of the Red Cross and Red Crescent reflects a more neutral approach, using the term “ICT activities” instead of “cyber operations”.[27] The experts of the Tallinn Manuals, for their part, use both the terms “cyber operation” and “cyber-attack”. While a cyber operation refers to “the employment of cyber capabilities with the primary purpose of achieving objectives in or by

---

11 UN GA. Resolution “Developments in the field of information and telecommunications in the context of international security”. URL: https://digitallibrary.un.org/record/399864?v=pdf (accessed: 07.12.2024).

12 The Tallinn Manual is a study without legally binding effect on the issue of the application of international law to “cyberspace”, which was prepared by an international group of experts from the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. There are two editions of the Tallinn Manual: of 2013 and 2017.

13 ICRC. International Humanitarian Law and Cyber Operations during Armed Conflicts, 2019. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (accessed: 17.11.2024).

14 Official Compendium of Voluntary National Contributions on the Subject of how International Law Applies to the Use of Information and Communications 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 Resolution 73/266 (hereinafter — Compendium). URL: https://digitallibrary.un.org/record/3933543 (accessed: 17.11.2024).

15 Ibid. P. 57.

16 Ibid. P. 79–83.

17 UNODA. Pakistan’s Position on the Application of International Law in Cyberspace, 3 March 2023 (hereinafter — the Official Position of Pakistan). URL: https://cyberlaw.ccdcoe.org/wiki/National_position_of_Pakistan_(2023) (accessed: 17.11.2024).

18 See the Compendium (Romania). P. 77–78.

19 Ibid. P. 85.

20 Ibid. P. 138–139.

21 Documento de posición de la república de Cuba sobre la aplicación del derecho internacional a las tecnologías de la información y comunicación en el ciberespacio. La Habana, 28 de junio de 2024 (hereinafter — the Official Position of Cuba). URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Documento_de_posición_de_Cuba._Aplicación_del_Derecho_Internacional_a_las_TIC_en_el_ciberespacio.pdf (accessed: 17.11.2024).

22 Ministry of Foreign Affairs of the Czech Republic. Czech Republic - Position paper on the application of international law in cyberspace, 27 February 2024 (hereinafter — the Official Position of the Czech Republic). URL: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf (accessed: 17.11.2024).

23 On the Application of International Law in Cyberspace: Position Paper, March 2021 (hereinafter — the Official Position of Germany).
URL: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed: 17.11.2024).

24 The Application of International Law to State Activity in Cyberspace (hereinafter — the Official Position of New Zealand). URL: https://www.dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace (accessed: 17.11.2024).

25 ICRC. International Humanitarian Law and Cyber Operations during Armed Conflicts, 2019. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (accessed 07.12.2024).

26 ICRC. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts – Recommitting To Protection In Armed Conflict On The 70th Anniversary Of The Geneva Conventions.
URL: https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf (accessed: 07.12.2024).

27 ICRC. Resolution ‘Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict’. URL: https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict (accessed: 07.12.2024).

the use of “cyberspace”,[28] a cyber-attack implies “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”.[29] For example, a cyber operation can be equated with the malicious use of ICTs (e. g. DDoS attacks or malware), however, a cyber-attack is an acute form of a cyber operation, requiring injury or death to persons or damage or destruction to objects. Therefore, not every cyber operation that is launched can be qualified as a cyber-attack. The author’s approach focuses on the use of cyber terminology for interpreting the concepts of IHL in the cyber context as well as for a more accurate and detailed assessment of the official positions of states which are accustomed to using such terminology.

2. Interpretation of the concepts of a military operation, an attack and an armed conflict in their application in the cyber context

There is currently no specific treaty dealing with the application of IHL to the malicious activities in “cyberspace”. Therefore, the further analysis will be based on the existing sources of IHL. Article 36 of the AP I stipulates a general rule in respect of new weapons according to which a state is obliged to determine whether their employment would be prohibited by the AP I or by any other rule of international law applicable to the state. This general rule is fully applicable to cybernetic activities. It means that states are under obligation to obey norms and principles of IHL when launching cyber-attacks against their adversaries in the context of an armed conflict.

As regards treaty interpretation, a general rule is contained in Article 31 of the Vienna Convention on the Law of Treaties (hereinafter — VCLT),[30] which establishes a cumulative three-tier test (wording, context and object and purpose) accompanied by the good faith principle for treaty interpretation.[31] Notwithstanding the fact that the AP I entered into force before the VCLT, the rule laid down in Article 31 reflects pre-existing customary international law.[32] Therefore, this rule of interpretation can be also applied to the provisions of the AP I.

2.1. Ordinary meaning of the concepts “military operation”, “attack”, “armed conflict”

First, the concept of “military operation” derives from Article 57 of the AP I, which is devoted to the protection of the civilian population and civilian objects during armed conflicts. The ICRC’s legal advisers have clarified the notion of military operation, which connotes “any movements, manoeuvres and other activities whatsoever undertaken by the armed forces with a view to combat”.[33] Hence, only if these rules are respected, civilians and civilian objects will not suffer in an armed conflict.

Second, the concept of “attack” derives from paragraph 1 of Article 49 of the AP I devoted to the definition of attack, which means “acts of violence against the adversary, whether in offence or in defence”. Consequently, such a definition has a broader meaning, covering defensive actions (in particular, “counterattacks”) as well as offensive actions, since both can affect the civilian population. In this respect, the term “attack” means “combat action”. In the *Milošević* case, the ICTY reiterated that any attack directed against civilians is prohibited, regardless of the military considerations that motivated it.[34] Furthermore, as noted in the *Kordic et Cerkez* case, in order to conclude that an “illegal attack on civilians” took place, it is not necessary that a certain number of civilians were killed or seriously injured but the number of civilian casualties may be relevant to conclude that the attack was illegal.[35] Within the meaning of the AP I, an attack is not related to the notion of aggression or the primary use of armed force since it refers only to the use of armed force to conduct a military operation at the beginning or during an armed conflict.[36] Thus, the concept of an attack is an acute form of a military operation that has consequences such as injury or death of people, as well as damage or destruction of military objectives.

---

28 Tallinn Manual. P. 15.
29 Ibid. P. 106.
30 Vienna Convention on the Law of Treaties (adopted on 23 May 1969, and entered into force on 27 January 1980).
31 *Vienna Convention on the Law of Treaties: A Commentary* / ed. by O. Dörr, Schmalenbach K. Heidelberg : Springer Berlin, 2018. P. 579–580.
32 Ibid. P. 561.
33 Commentary to the AP I. § 2189.
34 ICTY. *The Prosecutor v. Dragomir Milošević,* IT-98-29/1-T. Judgment of 12 December 2007. § 906.
35 ICTY. *The Prosecutor v. Kordic et Cerkez*, IT-95-14/2-A. Judgment of 17 December 2004. § 446.
36 International Committee of the Red Cross (ICRC). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Cambridge : Cambridge University Press, 1978 (hereinafter — Commentary to the AP I). § 1880–1882.

Third, there is the concept of "armed conflict", a definition of which has not been reflected in treaty law. The first paragraph of common Article 2 of the Geneva Conventions stipulates that they "shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them".[37] So the Geneva Conventions have defined the scope of their application, which is limited only to international armed conflicts.[38] However, the question of the definition of armed conflict is not addressed in the Conventions. The concept of armed conflict has been elaborated in case law, in particular in the *Tadić* case, in which the ICTY highlighted that "an armed conflict exists whenever there is a resort to armed force between states or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".[39] Moreover, in the *Limai* case, the ICTY underlined that there are two determinative elements of an armed conflict, meaning intensity of the conflict and the level of organisation of the parties, which distinguish an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities.[40] The ICC, for its part, pointed out in the *Bemba* case that "an international armed conflict exists in case of armed hostilities between States through their respective armed forces or other actors acting on behalf of the State".[41] Accordingly, the concept of an armed conflict refers to both international and non-international armed conflicts.

2.2. Applying an evolutionary method of interpretation in the cyber context

The author hypothesises that, in the context of emerging new means and methods of warfare, the concepts of "military operation", "attack" and "armed conflict" may evolve over time. In this respect, the changing ordinary meaning of the concepts of IHL plays a crucial role for the legal analysis of cyber-related issues. Generally, there are two theories of the treaty terms interpretation: static and evolutionary. The former ascribes to the legal text the normative meaning that it had at the time of its adoption, while the latter contemplates that the text should be interpreted so as to correspond to the normative meaning at the moment of interpretation.[42] The evolutionary method of interpretation is widely employed in jurisprudence of international courts. It was first applied in the case of *Tyrer v. the United Kingdom*, where the ECtHR held that "the Convention is a living instrument which… must be interpreted in the light of present-day conditions".[43] Then, in the case of *Christine Goodwin v. the United Kingdom*, the ECtHR clarified the concept of "present-day conditions" for the appropriate interpretation and application of the Convention for the Protection of Human Rights and Fundamental Freedoms.[44] In the *Costa Rica v. Nicaragua* case, the ICJ formulated a general rule as to when a treaty has an evolving meaning: (i) if the parties used "generic terms" when they were aware that the meaning of these terms was likely to change over time; (ii) if the treaty has been entered into for a very long period or is "of continuing duration".[45] Taking these approaches into account, and in the light of the rapid development of cyber technologies, an evolutionary method of interpretation can be deemed applicable for the interpretation of conventional concepts of IHL — a military operation, an attack, and an armed conflict — in the cyber context. Throughout its history, *jus in bello* has governed kinetic hostilities, however, the emergence of ICTs raises the question of applying traditional concepts to cybernetic activities. It seems justified to apply an evolutionary approach to the interpretation of the concepts of a military operation, an attack, and an armed conflict in relation to cyber activities, since the parties could have been aware of the evolving meaning of the "generic terms" used in the Geneva Conventions and Additional Protocols, and these treaties entered into force a long time ago. As a result, an evolutionary interpretation of the "generic terms" will encompass both kinetic and cybernetic activities carried out within an ongoing armed conflict.

According to M. Roscini, IHL applies to "cyberspace" in three scenarios: a) a cyber-attack is preceded by a declaration of war made using cybernetic or traditional means of communication; b) a cyber-attack occurs in the context of an ongoing international armed conflict and has a nexus with it; and c) a

---

37 International Committee of the Red Cross (ICRC). *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention).* 75 UNTS 135. 12 August 1949.

38 Only common Art. 3 of the Geneva Conventions is applicable to non-international armed conflicts.

39 ICTY. *The Prosecutor v. Dusko Tadic*, IT-94-1-A. Decision of 2 October 1995. § 70.

40 ICTY. *The Prosecutor v. Fatmir Limaj, Isak Musliu & Haradin Bala,* IT-03-66-T. Judgment of 30 November 2005. § 89.

41 ICC. *The Prosecutor v. Jean-Pierre Bemba Gombo*, ICC-01/05-01/08. Decision of 15 June 2009. § 223.

42 Spaic B. *Evolutionary and Static Interpretation //* Research Handbook on Legal Evolution / ed. by W. Załuski. Edward Elgar Publishing, 2023. P. 4.

43 ECtHR. *Tyrer v. the United Kingdom*. Application no. 5856/72. Judgment of 25 April 1978. § 31.

44 ECtHR. *Christine Goodwin v. the United Kingdom*. Application no. 28957/95. Judgment of 11 July 2002. § 84.

45 ICJ. *Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)*. Judgment of 13 July 2009. § 66.

cyber-attack amounts itself to an international armed conflict, with or without the concomitant occurrence of kinetic hostilities.[46] Thus, M. Roscini used an evolutionary approach to the interpretation of the first paragraph of common Article 2 of the Geneva Conventions. As practice shows, the most common case is when cyber-attacks are undertaken against the background of a pre-existing armed conflict. The frequency of this phenomenon is confirmed by a number of instances, including the use of cyber-attacks in the context of the Russia's special military operation,[47] the Israeli-Hamas conflict,[48] the Russian-Georgian conflict,[49] and the Armenian-Azerbaijani conflict.[50] Besides, cyber-attacks are often conducted in the absence of any armed conflict. This is evidenced by the case of the cyber-attack on Estonia[51] and the cyber-attack on the hospital in Düsseldorf, Germany.[52] Thus, apart from interpretation of the terms applied, it should be clarified whether there is customary international law regarding the application of IHL to cyber-attacks.

Using an evolutionary method of interpretation, the "generic terms" cover not only kinetic activities but also cybernetic ones. Therefore, pertinent provisions of the Geneva Conventions and Additional Protocols may be applied to cyber-attacks as well as to conventional weapons. Nowadays, military operations are conducted in a multitude of domains, i.e. on land, in sea, in the air, and in "cyberspace".[53]

2.3. Is there a rule of customary international law on the application of IHL to cyber-attacks?

A rule of customary international law consists of two constituent elements: state practice and *opinio juris*.[54] State practice must be general, which means it must be sufficiently widespread and representative, as well as consistent.[55] At the present time, not all states expressed their position on the application of international law to "cyberspace". Although a detailed assessment of national and common positions is made in the next part of the article, it should be noted that their small number does not allow to speak of the existence of a "general practice" since such practice is not representative (32 states out of 193 UN members). Also, state practice is not consistent, as evidenced by the diversity of the official positions of states as there are two "opposing camps of states": some of them are in favour of the full application of IHL to cyber-attacks, whereas others are sceptical about the application of IHL to cybernetic activities.[56] Additionally, China, Cuba, Pakistan, the Russian Federation, and the Syrian Arab Republic are acting as "persistent objectors" against the formation of customary international law on the issue of the application of IHL to "cyberspace" and, therefore, they are against the use of an evolutionary interpretation of the conventional concepts.

---

46 Roscini M. *Cyber Operations and the Use of Force in International Law*. Oxford : Oxford University Press, 2014. P. 120.

47 The Ministry of Digital Development, Communications and Mass Media of the Russian Federation reported massive DDoS attacks on the portal of public services from Ukraine. URL: https://tass.ru/ekonomika/15011477 (accessed: 17.11.2024).

48 Fowler J. *The Israeli-Hamas Conflict Shows Cyber Warfare Is Now the New Normal* // Website Planet. URL: https://www.websiteplanet.com/news/israel-palestine-cyberwarfare-report/ (accessed: 17.11.2024).

49 Mannes A., Hendler J. *The First Modern Cyberwar? //* The Guardian. 22 August 2008. URL: https://www.theguardian.com/commentisfree/2008/aug/22/russia.georgia1 (accessed: 07.05.2023).

50 Belovod'ev D. *Karabakhskaya voina khakerov: "raund" za Azerbaidzhanom [Karabakh Hacker War: the "Round" for Azerbaijan]* // Dailystorm. 29 July 2020. URL: https://dailystorm.ru/obschestvo/karabahskaya-voyna-hakerov-raund-za-azerbaydzhanom (accessed: 17.11.2024).

51 Ottis R. *Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective*. 7th European Conference on Information Warfare and Security 2008. ECIW, 2008. P. 163–168.

52 *Prosecutors Open Homicide Case after Cyber-attack on German Hospital* // The Guardian. 18 September 2020. URL: https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital (accessed: 17.11.2024).

53 Ardilla Castro C. A., Ramírez Benítez E., Cubides-Cárdenas J. *International Humanitarian Law and Its Significance for Current and Future Military Operations* // Revista Científica General José María Córdova. 2020. Vol. 32. № 18. P. 861.

54 Draft conclusions on identification of customary international law, adopted by the International Law Commission at its seventieth session, in 2018, and submitted to the General Assembly as a part of the Commission's report covering the work of that session. Conclusion 2.

55 Ibid. Conclusion 4.

56 For example, Cuba, Pakistan, the Russian Federation, and the Syrian Arab Republic. Declaration by M. Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 23 June 2017. URL: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf (accessed: 08.12.2024). See: A. V. Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, to a question from the TASS news agency about the state of international dialogue in this area. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1549172/ (accessed: 08.12.2024); UN GGE on Cybersecurity: The End of an Era? URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (accessed: 08.12.2024).

In terms of attacks, there are states stressing that a cyber-attack can, under certain circumstances, cross the threshold of an attack.[57] According to Canada, Denmark and Italy, the qualification of a cyber-attack as an attack requires injury or death to persons or damage or destruction to objects.[58] Germany, on the other hand, claims that the qualification of a cyber-attack as an attack in the sense of Article 49 of the AP I may not require the consequences comparable to effects of conventional weapons.[59] In practical terms, Israel considers that the operation aimed at cutting off electricity in a military airfield, and which is expected to cause the crash of a military aircraft, may constitute an attack.[60] Therefore, at least several states recognise a possibility of qualifying a cyber-attack as an attack in the meaning of Article 49 of the AP I.

With regard to the concept of armed conflict, a limited number of states out of those who have expressed their position on the applicability of international law in the ICTs environment allowed for the possibility of qualifying a cyber-attack as an armed conflict. For example, Brazil recognises that the cyber activities can constitute an armed conflict, should they themselves cross the threshold of violence.[61] In such a case a cyber-attack can be a prerequisite for the outbreak of hostilities.

To sum up, first, the ordinary meaning of the concepts “military operation”, “attack”, “armed conflict” implies their application only to kinetic activities; second, an evolutionary interpretation of the terms allows them to include cybernetic activities; third, there is no rule of customary international law on how international law should in principle apply to “cyberspace” and, in particular, to what extent IHL applies to the malicious use of ICTs.

3. Classification of the official positions of states on the application of IHL to “cyberspace”: in search of a consensus

Two paradigms can be developed from the states’ positions on the issue of the application of IHL to “cyberspace”: absolute and limited. The former aims at expanding the ambit of IHL norms in “cyberspace” and, as a result, the applicability of *jus in bello* becomes possible not only in the context of an armed conflict but also long before it, since a cyber-attack *per se* constitutes an attack or even an armed conflict. The latter is devoted to the restrictive application of IHL norms to “cyberspace” only in the case of armed conflict, where cyber-attacks act as a means or method of warfare.

The official positions of states on the applicability of international law to “cyberspace” were reflected, in particular, in the “Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States”, which was prepared by the Group of Governmental Experts in accordance with GA resolution 73/266. This collection is composed of stances of 15 states: Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, the Netherlands, Norway, Romania, the Russian Federation, Singapore, Switzerland, the UK, and the USA.[62] So they have voluntarily expressed their vision of the application of international law to the use of ICTs, covering different areas: from countermeasures and international humanitarian law to human rights and sovereignty issues. In addition, several positions can be found on the official websites of national governments.

To date, there are 32 national positions and two common positions on the issue of the application of international law to the ICTs environment, with 30 states and two unions expressing their explicit position on the application of IHL to “cyberspace”. For instance, the positions of the Islamic Republic of Iran[63] and

---

[57] This group of states includes Australia, Canada, the Czech Republic, France, Germany, Denmark, Israel, Italy, Japan, New Zealand, Norway, the Netherlands, Pakistan, Sweden, Switzerland, the UK, and the USA.

[58] See e.g., International Law applicable in cyberspace (hereinafter — the Official Position of Canada). URL: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng (accessed: 17.11.2024); Government of Denmark. Denmark’s Position Paper on the Application of International Law in Cyberspace, 4 July 2023 (hereinafter — the official position of Denmark). URL: https://brill.com/view/journals/nord/92/3/article-p446_007.xml (accessed: 17.11.2024); International law and cyberspace (hereinafter — the official position of Italy).
URL: https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf (accessed: 17.11.2024).

[59] See the Official Position of Germany. P. 8.

[60] Schondorf R. *Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations* // International Law Studies. 2021. Vol. 97. № 395. P. 400.

[61] See the Compendium (Brazil). P. 17.

[62] See the Compendium.

[63] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the “Cyberspace”, August 2020 (hereinafter — the Official Position of Iran). URL:

the People's Republic of China[64] are silent on the abovementioned matter. However, the Islamic Republic of Iran affirmed that cyber operations that result in widespread and serious material damage to property and/or persons and/or logically capable of leading to such consequences constitute the "use of force",[65] but this statement refers to *jus ad bellum*.

Still, owing to the efforts of the United Nations, a certain compromise has been reached on whether *jus in bello* norms apply to the use of ICTs by states and, if so, in which cases. The consensus is that IHL partially applies to the use of ICTs by states only in situations of armed conflict. Moreover, states who have expressed their opinion on the matter have confirmed the applicability of the basic principles of IHL to "cyberspace", such as humanity, necessity, proportionality, and distinction.[66]

All the official positions of states could be classified on two grounds. The first classification of states includes those that agree with the applicability of IHL norms to "cyberspace" only in the event of an armed conflict, as well as those who agree to the application of IHL norms in the absence of an armed conflict but emphasise that the cyber-attack itself may be a prerequisite for the outbreak of hostilities. The first group (confirming the application IHL to the use of ICTs in the event of armed conflict) consists of the African Union,[67] Cuba,[68] Estonia,[69] Kazakhstan,[70] Kenya,[71] Pakistan,[72] Poland,[73] Romania,[74] the Russian Federation,[75] and Singapore.[76] The second group (consenting on the application of IHL to cyber-attacks when they themselves amount to an attack or an armed conflict) includes Austria,[77] Brazil,[78] Canada,[79] the Czech Republic,[80] Denmark,[81] Italy,[82] Japan,[83] Israel,[84] France,[85] Costa Rica,[86] Finland,[87] Ireland,[88] the UK,[89]

https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat (accessed: 17.11.2024).

64 China's Positions on International Rules-making in Cyberspace (hereinafter — the Official Position of China). URL: https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405183.html (accessed: 17.11.2024).

65 See the Official Position of Iran. Article IV.

66 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. URL: https://digitallibrary.un.org/record/3934214?v=pdf (accessed: 09.12.2024).

67 African Union Peace and Security Council. Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024 (hereinafter — the Official Position of the AU). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4714756 (accessed: 17.11.2024).

68 See the Official Position of Cuba.

69 See the Compendium (Estonia). P. 26–27.

70 Ibid. P. 51.

71 Ibid. P. 53. Unlike other members of the African Union, Kenia has separately expressed its position in the Compendium.

72 See the Official Position of Pakistan.

73 Ministry of Foreign Affairs of Poland. The Republic of Poland's position on the application of international law in cyberspace, 29 December 2022 (hereinafter — the Official Position of Poland). URL: https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Republic_of_Poland_(2022) (accessed: 17.11.2024).

74 See the Compendium (Romania). P. 77–78.

75 Ibid. P. 79–83.

76 See the Compendium (Singapore). P. 85.

77 See the Official Position of Austria.

78 See the Compendium (Brazil). P. 17.

79 See the Official Position of Canada.

80 See the Official Position of the Czech Republic.

81 See the Official Position of Denmark.

82 See the Official Position of Italy.

83 See the Compendium (Japan). P. 45–50.

84 Schondorf R. *Op. cit*. P. 395–406.

85 Ministère des Armées (France): Manuel de droit des opérations militaires (hereinafter — the Official Position of France). URL: https://www.defense.gouv.fr/sites/default/files/sga/Manuel%20de%20droit%20des%20opérations%20militaires_édition%202022.pdf (accessed: 17.11.2024).

86 Ministry of Foreign Affairs of Costa Rica. Costa Rica's Position on the Application of International Law in Cyberspace, 21 July 2023 (hereinafter — the Official Position of Costa Rica). URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf (accessed: 17.11.2024). Page?

87 Finland's National Positions. International Law and Cyberspace, 2020 (hereinafter — the Official Position of Finland). URL: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed: 07.05.2023).

88 Ireland: Position Paper on the Application of International Law in Cyberspace (hereinafter — the Official Position of Ireland). URL: https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf (accessed: 17.11.2024).

89 See Compendium (the UK). P. 118–119.

Germany,[90] the European Union,[91] New Zealand,[92] Norway,[93] the Netherlands,[94] Sweden,[95] Switzerland,[96] Australia,[97] and the USA.[98]

The second classification is based on the qualification of a cyber-attack either as an attack or as an armed conflict. Consequently, states can be divided into (i) those that have stated that a cyber-attack can reach the threshold of an attack, and (ii) those that have indicated that a cyber-attack can reach the level of an armed conflict *per se*. Accordingly, the "attack" group includes Australia, Austria, Canada, the Czech Republic, the European Union, Germany, Denmark, Israel, Italy, Japan, New Zealand, Norway, the Netherlands, Sweden, Switzerland, France, the UK, and the USA. The "armed conflict" group consists of Brazil, Costa Rica, Ireland, and Finland. It is important to note that, in the opinion of most states, a cyber-attack must necessarily cause either death or harm to individuals or physical damage to objects. Furthermore, some states that have resorted to cyber-attacks in the context of armed conflicts have not prepared their position papers, referring to Azerbaijan, Armenia, Georgia, and Ukraine.

As an intermediate conclusion, it should be emphasised that a cyber-attack can be qualified as a military operation, an attack, and an armed conflict, based on the stances of those states that have taken a position on the application of IHL to "cyberspace". It follows that there is fragmentation in state practice since current official positions are classified into two "opposing camps": absolute and limited paradigms on the issue of the application of IHL to the use of ICTs. As noted earlier, there is no rule of customary international law. Therefore, the position of the majority of states, which allows the qualification of cyber-attacks as an attack and armed conflict, does not constitute a legally binding rule for the entire international community. In fact, the current norm-setting process is in a sense "on thin ice". In this respect, "stretching" *jus in bello* to cybernetic activities creates threats for the international community due to prospective militarisation of "cyberspace".

4. The "Sisyphean task" or the recognition of data as an object under IHL

As mentioned in the introduction, personal data is often the target of a cyber-attack. In this regard, the debate on the recognition of data as an "object" under IHL contributes to the understanding of how and why states (adherents of the absolute paradigm) qualify cyber-attacks as a military operation, an attack, and an armed conflict. Thus, the legal qualification of cyber-attacks depends on whether and to what extent states recognise data as an "object" under IHL. This part of the study discusses theoretical approaches and official positions on the question of whether data should be considered an object under IHL. It is highly important to address this issue as "attacks" are generally allowed only against military objectives.

At the present time, there are three key approaches to the qualification of data as an object under IHL: literal, analogist, and functional.[99] Out of 30 states which commented on the application of IHL to "cyberspace", only 11 have addressed the issue of qualifying data as an object under IHL. It follows that state practice concerning the recognition of data as an object under IHL is scarce. Furthermore, there is no universal vector on this question, even within the states belonging to the single camp (adherents of the absolute paradigm).

---

90 See the Official Position of Germany.

91 Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace (hereinafter — the Official Position of the EU).
URL: https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf (accessed: 09.12.2024).

92 See the Official Position of New Zealand.

93 See Compendium (Norway). P. 74–75.

94 Ibid. P. 59–60.

95 Government Offices of Sweden, Position Paper on the Application of International Law in Cyberspace, July 2022. URL: https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Kingdom_of_Sweden_(2022) (accessed: 17.11.2024) (hereinafter — the Official Position of Sweden).

96 Federal Department of Foreign Affairs. Switzerland's Position Paper on the Application of International Law in Cyberspace, May 2021 (hereinafter — the Official Position of Switzerland).
URL: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf (accessed: 17.11.2024).

97 Australia's Submission on International Law to be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber (hereinafter — the Official Position of Australia).
URL: https://ccdcoe.org/uploads/2018/10/Australia_submission-on-international-law-to-be-annexed-to-the-report-of-the-2021-Group-of-Governmental-Experts-on-Cyber.pdf (accessed: 17.11.2024).

98 Ibid. P. 138–139.

99 Mačák K. *Unblurring the Lines: Military Cyber Operations and International Law* // Journal of Cyber Policy. 2021. Vol. 6. № 3. P. 421–422.

4.1. The literal interpretation of the concept “object” under IHL

In fact, the recognition of data as an object is not directly regulated by IHL. Nevertheless, the ordinary meaning of the concept “object” is derived from the provisions of the AP I and its Commentary. Article 48 of the AP I envisages a distinction principle according to which the belligerents are under obligation to distinguish between the civilian population and combatants as well as between civilian objects and military objectives.[100] Paragraph 2 of Article 52 of the AP I clarifies what military objectives are by providing a two-tier test: (i) their nature, location, purpose or use make an effective contribution to military action; (ii) their total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.[101] The definition of a civilian object is derived from the absence of features of a military objective, meaning “presumption of civilian nature”.[102]

In addition, the AP I specifies that attacks within the meaning of Article 48 must be strictly limited to military objectives. In this respect, it is worth analysing the ordinary meaning of the concept of “object” under IHL. The interpretation of this concept can be found in the Commentary to the AP I of 1978. The authors of the Commentary note that the term “object” means “something that is visible and tangible”, based on the content of the English (“object”) and French (“bien”’) texts of the AP I.[103] Thus, data is not “object” under IHL based on literal interpretation of the AP I. Among the commentators, O. Pomson contends that the term “object” refers to material things under customary international law and therefore computer data cannot be regarded as an object under IHL.[104] M. N. Schmitt prefers to exclude data *per se* from the concept of an object under IHL stressing that the belligerents often use cyber psychological operations, which are aimed at destroying or altering data and disrupting civilian media activities.[105] It seems therefore, that it is impossible to qualify a cyber-attack on personal data as an attack in the meaning of Article 48 of the AP I since it can only be directed against tangible and visible things which, according to the distinction principle, meet the requirements of a military objective. However, those states that qualify cyber-attacks on personal data as attacks in the meaning of Article 48 of the AP I use other tools of the interpretation, such as analogist and functional theories.

4.2. The analogist and functional approaches to the interpretation of the term “object”

The analogist approach is based on the application of analogy in international law,[106] in particular with respect to the law of targeting. This theory is maintained by ICRC’s legal advisers. The “guardians of IHL” are convinced that the protection of civilian data from cyber-attacks in the context of armed conflict is becoming an increasingly urgent problem. The resolution of the 34th International Conference of the Red Cross and Red Crescent expressed a deep concern about data protection from malicious ICT activities.[107] The resolution also addresses the protection of humanitarian data.[108]

Some ICRC’s legal advisers contend that data is an essential component of the digital sphere and a cornerstone of life in many communities, concerning personal medical data, social insurance data, tax reports, bank accounts.[109] The ICRC’s legal advisers apply the term “civilian data” in respect of personal data.[110] In this regard, the norms of the law of targeting should also be applied to civilian data as cyber-attacks leading to the disruption of public services and private businesses can cause more damage to the civilian population than the destruction of physical objects.[111] Furthermore, a narrow definition of

---

100 See the AP I.
101 Ibid.
102 David E. *Printsipy prava vooruzhennykh konfliktov* [*Principles of the Law of Armed Conflict*], Moscow: The ICRC, 2011. P. 284.
103 Commentary to the AP I. § 2008.
104 Pomson O. ‘*Objects’? The Legal Status of Computer Data under International Humanitarian Law* // Journal of Conflict and Security Law. 2023. Vol. 28. № 2. P. 380.
105 Schmitt M. N. *Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations* // International Review of the Red Cross. 2019. Vol. 101. № 910. P. 342.
106 Vöneky S. *Analogy in International Law* // Max Planck Encyclopedia of Public International Law / ed. by R. Wolfrum. Oxford : Oxford University Press, 2008.
107 ICRC. Resolution ‘Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of ICT Activities During Armed Conflict’.
URL: https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict (accessed 07.12.2024).
108 Ibid.
109 Laurent G., Tilman R., Knut D. *Op. cit.* P. 20.
110 Ibid.
111 ICRC. International Humanitarian Law and Cyber Operations during Armed Conflicts, 2019.
URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (accessed 17.11.2024).

"civilian objects" under IHL would expose a legal *lacuna* in order to protect civilian data or personal data.[112] Most of states that commented the issue of recognising data as an object under IHL are supporting the analogist approach, including Austria,[113] Brazil,[114] Costa Rica,[115] Finland,[116] France,[117] Germany,[118] Norway,[119] Romania,[120] Switzerland.[121] To illustrate, France states that content data (civilian, medical or bank) is protected under the distinction principle.[122] According to Romania, cyber-attacks can only be directed against that data which qualifies as military objectives.[123] This approach is mainly based on policy considerations rather than on existing legal norms governing the issue of targeting. The author acknowledges that such an approach can be justified on the grounds of special protection of civilian and humanitarian data. The scope of the discussion depends on the political views of each state, however, it goes beyond the *lex lata*.

Another approach is functional; its adherents are experts of the Tallinn Manuals. They unanimously agree that computers, computer networks and other material components of the cyber infrastructure may be considered objects under the law of targeting.[124] Nevertheless, their opinions on the legal status of the data were divided. The position of most experts focuses on the fact that the ordinary meaning of the term "object", which was discussed in the Commentary to the AP I, cannot be interpreted as data-related since objects are visible and tangible.[125] In contrast, others have stated that either all or some types of data should be considered as an object under IHL. Therefore, the "modern meaning" of the notion of the object in society and its interpretation in the light of object and purpose of the AP I should lead to the conclusion that data is an object for the purposes of the law of targeting.[126] It is worth noting that experts agreed that any cyber-attack conducted against data with the expected injury or death to people, as well as damage or destruction of objects, would constitute an attack, to which targeting rules apply.[127] Accordingly, cyber-attacks against data would not fall within the scope of the relevant norms of IHL unless the attack in question resulted in some physical effect and/or loss of functionality of the target system or network.[128] The functional approach was reflected in the official positions of Chile,[129] Denmark,[130] and Israel.[131] For instance, Denmark emphasises that an operation targeting data on which the functionality of an object depends can be considered an attack, depending on the nature and degree of damage that is expected to result from this operation.[132] This approach seems to be dangerous for the qualification of data as an object under IHL, as it aims at the militarisation of "cyberspace" which is expressed in the fact that a cyber-attack on personal data resulting in some physical effect and/or loss of functionality of the target

---

112 Horowitz J. *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*. ASIL Insights, 19 May 2020. URL: https://www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc (accessed: 17.11.2024).

113 See the Official Position of Austria.

114 See Compendium. P. 22–23.

115 See the Official Position of Costa Rica.

116 See the Official Position of Finland.

117 See the Official Position of France.

118 See the Official Position of Germany.

119 Norway, Manual i krigens folkerett, 2013. URL: https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/194213/manual_krigens_folkerett.pdf?sequence=1&isAllowed=y (accessed: 17.11.2024).

120 See Compendium (Romania). P. 78.

121 See the Official Position of Switzerland.

122 See the Official Position of France.

123 See Compendium (Romania). P. 78.

124 Tallinn Manual. P. 124-125.

125 Commentary to the AP I. § 2007–2008.

126 Mačák K. *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law* // Israel Law Review. 2015. Vol. 48. № 1. P. 80.

127 McCormack T. *International Humanitarian Law and the Targeting of Data* // International Law Studies. 2018. Vol. 94. № 1. P. 222–240.

128 Schmitt M. N. *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*. 2nd ed. Cambridge : Cambridge University Press, Cambridge. 2017 (hereinafter — Tallinn Manual 2.0). P. 437.

129 Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS, Improving Transparency: International Law and State Cyber Operations: Fifth Report. URL: https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf (accessed: 17.11.2024).

130 Ministry of Defence of Denmark. Military Manual on International Law Relevant to Danish Armed Forces in International Operations, 2016 (hereinafter — the Official Position of Denmark). URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/DK-Military-Manual-International-Operations.pdf (accessed: 17.11.2024).

131 Schondorf R. *Op. cit*. P. 401.

132 See the Official Position of Denmark.

system or network will constitute an attack (a defensive or offensive act of violence against the adversary).

Applying the above approaches to the question of qualifying cyber-attacks on personal data, the following conclusions on potential scenarios can be drawn.

The first scenario: if the state does not consider personal data to be an object under IHL, then cybernetic activities against such data would not constitute a gross violation of IHL. Since data is not an "object" for the purposes of IHL, it does not have to meet the criteria of a military objective for a cyber-attack against it to be legal under IHL.[133] This case illustrates a "gray zone" of modern IHL.

The second scenario: if the state admits that a sensitive type of data (civilian and humanitarian) can be an "object" under IHL, then in the case of a cyber-attack on this type of data, the state will probably speak of a grave breach of IHL, since this data is recognised as a civilian object. Thus, cyber-attacks on this type of data are prohibited.

The third scenario: if the state considers that a cyber-attack can have consequences in the form of physical damage to network systems, this state recognizes that data can qualify as an "object", but its nature (civilian or military) depends on the circumstances. Therefore, such "cyber-attacks" can be permissible insofar as this data meets the criteria of the definition of a military objective.[134]

To sum up, the most appealing approach to the question of the data qualification is a literal interpretation, as it is based on the existing targeting norms (*lex lata*), which clarify that "objects" under IHL are things that can be touched and seen. Applying such an approach, it can be concluded that there is no option to qualify cyber-attacks on personal data under IHL. Therefore, this approach does not answer the research question. However, drawing on other theories of data qualification, there are two ways of interpreting the notion of "object" broadly through the lens of policy considerations and legal gaps (*lex ferenda*). The author agrees with the position of the ICRC's legal advisers, who argue for the protection of civilian and humanitarian data from cyber-attacks in times of armed conflicts. Nevertheless, based on the analogist approach, personal data as a civilian object will be under the general protection against any attack (including cybernetic). Thus, only in the context of application of the functional approach cyber-attacks launched on personal data may constitute an attack under certain conditions, including implications in the form of physical effect and/or loss of functionality of the target system or network. It should be noted that there is no consensus on the norm-setting concerning the recognition of data as an object under IHL in the official positions of states. Even those who adhere to the absolute paradigm take different positions. However, the majority of them support the application of the analogist approach in order to protect sensitive types of data in the event of armed conflict.

5. Potential scenarios for qualifying cyber-attacks on personal data: skating on thin ice

This part of the study is devoted to a range of potential scenarios in which cyber-attacks on personal data can be qualified as a military operation, an attack, and an armed conflict. For the purposes of this section, the functional approach should be applied, as it allows for the possibility of qualifying cybernetic actions on personal data (immaterial thing) as kinetic. Thus, three options for qualifying cyber-attacks on personal data are examined: a military operation, an attack, and an armed conflict.

The first option is a military operation, which means all movements, manoeuvres and other activities of any kind undertaken by the armed forces with a view to combat. In this case, cyber-attacks of any kind launched by the armed forces in order to conduct combat operations in the event of an armed conflict, alongside conventional weapons. For example, in the context of an armed conflict, state B launches a cyber-attack on the data systems of the Ministry of Defense (military objective), resulting in the deletion of records containing information on military strategy (military data). Such a cyber-attack can be considered a military operation. Therefore, cyber-attacks can be equated with the use of conventional weapons. In this respect, the use of malicious ICTs in the event of armed conflict must comply with the basic principles of IHL, such as necessity, humanity, distinction and proportionality. Nevertheless, a cyber-attack directed against hospitals or schools containing civilian data would constitute a grave violation of the principle of distinction.

---

[133] Scenario 12: Cyber operations against computer data.
URL: https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data (accessed: 10.12.2024).

[134] Ibid.

Another instance is a situation where state N carries out a cyber-attack on the building of state M where both the personal data of civilians and the military data is stored, resulting in the deletion of the data of some civilians. Accordingly, this cyber-attack will be assessed according to the principle of proportionality: whether the military advantage outweighs the damage to the civilian object (the deletion of civilian data). In order to qualify a cyber-attack on personal data as a military operation, the most important element is the *context criterion* that must be met. The experts of the Tallinn Manuals understand the "context" as the concept that refers either to the fact that operations are conducted by the belligerent against the enemy or that they are conducted to facilitate the military efforts of the belligerent.[135] Another criterion is the *nexus* between cybernetic activity and armed conflict. By way of illustration, Austria considers that there must be a sufficient nexus of cybernetic activity and armed conflict, meaning a cyber-attack is carried out by one party to the conflict against the other, and which must contribute to the military efforts of the former.[136] Thus, two criteria for qualifying cyber-attacks on personal data as a military operation can be developed: context and nexus.

The second option is an attack which implies defensive or offensive acts of violence against the enemy in the meaning of Article 48 of the AP I. For example, in the absence of an armed conflict, the armed forces of state A conduct an offensive cyber-attack against the industrial control systems of a wastewater treatment plant in state B, altering critical data sets necessary to maintain the correct level and composition of chemicals for the treatment of drinking water in a large city.[137] This cyber-attack may qualify as an attack since it results in the shutdown of the facility, i.e. the damage to the civilian object. Therefore, this cyber-attack is not permitted as it is directed against the civilian object. Besides, the experts of the Tallinn Manuals consider that a cyber-attack that causes a fire at a small military objective would be enough to commence an international armed conflict.[138] As a real-life example it is worth recalling a situation when the air strike by Israel in 2019 targeting a building in Gaza in response to a possible cyber-attack carried out by the group Hamas.[139] This was the first time that the alleged cyber-attack was accompanied by a real kinetic attack on the object. Another illustrative example is the case of the Düsseldorf hospital where a patient died as a result of a cyber-attack. The hospital was unable to admit her because its systems had been knocked out by a cyber-attack, involving the use of ransomware. German prosecutors then began investigating the patient's murder.[140]

Based on the official positions of states, the main criterion for qualifying a cyber-attack as attack is the consequences in the form of injury or death of people, as well as damage or destruction of objects. Accordingly, whenever an attack on data results in injury or death of individuals or damage or destruction of physical objects, these persons or objects become the "target of attack". Furthermore, a cyber-attack on data upon which the functionality of physical objects depends sometimes constitutes an attack.[141] This approach is followed by the majority of states that have chosen the absolute paradigm (Australia, Brazil, Canada, Costa Rica, the Czech Republic, Denmark, the European Union, Finland, France, Germany, Ireland, Israel, Italy, Japan, New Zealand, Norway, the Netherlands, Pakistan, Sweden, Switzerland, the UK, and the USA). To give an example, Canada states that injury or death to persons or damage or destruction to objects includes harmful effects above a *de minimis* threshold on cyber infrastructure, or the systems that rely on it.[142] Interestingly, there is a link between the official positions on the application of IHL to "cyberspace" and on the recognition of data as an object under IHL. Thus, Denmark and Israel follow the functional approach (partially recognising data as an object under IHL), while at the same time allowing for the possibility of qualifying a cyber-attack on personal data as an attack. Thus, the following criterion for qualifying a cyber-attack on personal data as an attack can be developed: the consequences in the form of injury or death of people, as well as damage or destruction of objects. The main problem

---

135 Tallinn Manual. P. 96–97.
136 See the Official Position of Austria.
137 Geiss R., Lahmann H. *Protection of Data in Armed Conflict* // International Law Studies. 2021. Vol. 97. № 556. P. 558.
138 Tallinn Manual 2.0. P. 383.
139 Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. URL: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroyshamas-cyber-hq-in-world-first/?sh=29a9597fafb5 (accessed: 10.12.2024).
140 Prosecutors Open Homicide Case After Cyber-Attack on German Hospital. URL: https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital (accessed 17.11.2024).
141 Tallinn Manual 2.0. P. 416.
142 See the Official Position of Canada.

with such a qualification, however, is that it leaves open the possibility that a cybernetic activity could lead to a kinetic one, as has been demonstrated in the case of Israel.

The third option is an armed conflict, which is quite challenging to prove. In this case, a cyber-attack *per se* crosses the threshold of violence. The threshold of violence in international armed conflict is low, while it is very high in the context of a non-international armed conflict. In the current time, only four states allow the possibility of characterising a cyber-attack as an armed conflict: Brazil, Costa Rica, Finland, and Ireland. For instance, Finland emphasises that in assessing the cyber-attack it is necessary to know whether it causes prohibited harm, including foreseeable direct and indirect effects.[143] Moreover, in Ireland's view, cyber-attacks must have effects similar to those of physical military operations constituting armed force in order to bring into existence (i) an international armed conflict if they are conducted between states, and (ii) can bring into existence a non-international armed conflict if the two requirements of intensity of conflict and level of organisation are met.[144] It is worth noting that history does not yet know examples where a cyber-attack was considered a precondition for an armed conflict. Thus, the main criterion for qualifying a cyber-attack as an armed conflict is the crossing by this cybernetic activity of the threshold of violence, which is different for an international and non-international armed conflicts.

To summarise, a cyber-attack on personal data can be qualified as a military operation, an attack, and an armed conflict according to the following criteria: (i) the context and nexus (a military operation); (ii) consequences in the form of injuries or deaths, damage, or destruction of objects (an attack); (iii) a threshold of violence (an armed conflict). As a result, the easiest option of the qualification is the first scenario when a cyber-attack is carried out as part of an ongoing armed conflict. Regarding the second scenario, it is worth noting that state practice on such a qualification is scarce. The last option of the qualification is really dangerous within the framework of modern IHL since it leads to the militarisation of "cyberspace" that is accompanied by transformation of contemporary armed conflicts.

6. Comparing positions of the Russian Federation and the United States

First of all, it should be emphasised that neither the Russian Federation nor the United States expressed their position on the issue of the recognition of data as an object under IHL. Nevertheless, these states commented on the application of IHL to "cyberspace".

Basically, the Russian Federation and the United States hold opposing positions on the question of application of IHL to the use of ICTs. On the one hand, Russia pays attention to the fact that the humanitarian aspects of information security and the ethics of its use are becoming the most important elements of global, national, public and personal security in the modern world. The Russian Federation supports a "window of opportunity" to conclude new treaties to strengthen international information security.[145] However, its position is silent on the issue of data protection, especially in times of armed conflict. In general, Russia is a proponent of the limited paradigm, which means that it considers that IHL applies to the use of ICTs only in the case of armed conflict.

The United States, on the other hand, is an adherent to the absolute paradigm, i.e. it advocates "stretching" the scope of IHL to cyber-attacks carried out in the absence of hostilities. By way of illustration, in his remarks of 10 November 2016, US legal adviser B. Egan stated that, although "not all cyber operations rise to the level of an 'attack' as a legal matter under the law of armed conflict", it is nevertheless possible to determine such cyber operation as an attack, "considering, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question".[146] Therefore, the representatives of the United States opined that the criterion of kinetic effects was not relevant in respect of the qualification of a cyber-attack as an attack. When comparing two positions of the states concerned it should be noted that emphasising that these are "headliners" in the application of international law in general: while the Russian Federation expresses mainly its concerns on

[143] See the Official Position of Finland.
[144] See the Official Position of Ireland.
[145] Ministry of Foreign Affairs of the Russian Federation. Interview of the Director of the Department of International Information Security of the Russian Foreign Ministry A.V. Krutskikh. *Global Cyber Warfare: a Diplomatic Victory* // International Life. 7 June 2021. URL: https://www.mid.ru/ru/foreign_policy/un/1752094/ (accessed: 17.11.2024).
[146] Egan B. *Remarks on International Law and Stability in Cyberspace*. Speech at Berkeley Law School, 10 November 2016. URL: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm (accessed: 17.11.2024).

the of criminalisation of cybernetic activities (criminal lawmaking track), the United States focuses on "stretching" modern *jus in bello* to non-kinetic (cybernetic) activities (military lawmaking track).

Concluding remarks

Answering the first part of the research question, it should be noted that a cyber-attack on personal data may qualify as a military operation, an attack and even an armed conflict. This qualification is possible if this cyber-attack meets certain requirements. As a result, the author has developed the following criteria: (i) the context and nexus (a military operation); (ii) consequences in the form of injuries or deaths, damage, or destruction of objects (an attack); (iii) a threshold of violence (an armed conflict). Furthermore, the author concludes that the qualification of cyber-attacks on personal data depends on the state's position on the issue of recognising data as an object under IHL, as demonstrated by the examples of Denmark and Israel.

For the purposes of the study, an evolutionary approach has been used to interpret the conventional concepts since the ordinary meaning of the terms does not allow their application to cybernetic activities. Based on the analysis of the current official positions of states on the issue of the application of IHL to "cyberspace", there is fragmentation in state practice, since current official positions are classified into two "opposing camps": absolute and limited paradigms. Besides, there is no rule of customary international law as the position of those states, who allow the qualification of cyber-attacks as an attack and armed conflict, does not constitute a legally binding rule for the entire international community.

Moreover, since the literal interpretation of the provisions of the AP I clarifies that an object under IHL is something that can be seen and touched, data is not included in this meaning (*lex lata*). However, based on policy considerations, it appears the position in favour of protecting a sensitive type of data (e.g. civilian and humanitarian) from cyber-attacks in times of armed conflicts (*lex ferenda*) is justified. Thus, a literal interpretation of the concept of object under IHL creates a "grey area", as there is no legal protection for civilian and humanitarian data that may be disrupted in the event of armed conflict. It is worth mentioning the "Martens clause", which remains applicable in any event where IHL is silent, and which could fill the legal *lacunas* in the protection of sensitive types during armed conflicts.

Overall, the author is convinced that "stretching" *jus in bello* to activities carried out in "cyberspace" creates threats for the international community if a cyber-attack can be qualified as an attack or can serve as a precondition for the outbreak of kinetic hostilities. Those states that adhere to the absolute paradigm contribute to the militarisation of "cyberspace", i.e. its transformation into a new domain of hostilities.

ПО ТОНКОМУ ЛЬДУ: КВАЛИФИКАЦИЯ КИБЕРАТАК НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СООТВЕТСТВИИ С МЕЖДУНАРОДНЫМ ГУМАНИТАРНЫМ ПРАВОМ

АБРАШИН Р. П.

Абрашин Роман Петрович — младший юрист, Центр международного права на Чистых прудах, Москва, Россия (rpabrashin@gmail.com). ORCID: 0000-0003-4891-359X.

Аннотация

В статье анализируется возможность и обстоятельства квалификации кибератак на персональные данные с точки зрения международного гуманитарного права (далее — МГП). Автор рассматривает три варианта квалификации кибератак на персональные данные: военная операция, нападение и вооруженный конфликт. Часто именно персональные данные становятся объектом кибератаки. Ввиду этого обстоятельства дискуссия о признании данных «объектом» в соответствии с МГП способствует решению вопроса о юридической квалификации кибератаки, которая зависит, в частности, от того, признают ли государства данные «объектом» в соответствии с МГП, и в какой степени. В отсутствие международного договора, регулирующего применение МГП к злонамеренному использованию ИКТ, основное внимание в исследовании уделяется существующим источникам МГП (Женевским конвенциям, Дополнительным протоколам, принципам), международному обычному праву, а также судебным решениям и правовым доктринам, выступающим вспомогательным средством определения правовых норм. Особое внимание уделяется позициям Российской Федерации и Соединенных Штатов по вопросу о применении МГП к кибернетической деятельности. В результате автор приходит к выводу, что кибератака на персональные данные может квалифицироваться как военная операция, нападение и предпосылка вооруженного конфликта, и предлагает возможные критерии для такой квалификации. Автор убежден, что распространение *jus in bello* на кибернетическую деятельность создает угрозы для международного сообщества ввиду потенциальной милитаризации «киберпространства».

Ключевые слова

кибератака, *jus in bello*, нападение, вооруженный конфликт, персональные данные

Для цитирования: Абрашин Р. П. *По тонкому льду: квалификация кибератак на персональные данные в соответствии с международным гуманитарным правом* // Журнал ВШЭ по международному праву (HSE University Journal of International Law). 2024. Т. 2. № 4. С. 36–52.

https://doi.org/10.17323/jil.2024.24743

References / Список источников

Ardilla Castro C. A., Ramírez Benítez E., Cubides-Cárdenas J. (2020) International Humanitarian Law and Its Significance for Current and Future Military Operations. Revista Científica General José María Córdova, vol. 18, no. 32, pp. 857–882.

Chang Z. (2017) Cyberwarfare and International Humanitarian Law. Creighton International and Comparative Law Journal, vol. 9, no. 1, pp. 29–53.

David E. (2011) Printsipy prava vooruzhennykh konfliktov [Principles of the Law of Armed Conflict], Moscow: The ICRC.

Dörr O., Schmalenbach K. (eds.) (2018). Vienna Convention on the Law of Treaties: A Commentary, Heidelberg: Springer Berlin.

Garkusha-Bozhko S. Yu. (2021) Mezhdunarodnoe gumanitarnoe pravo v kiberprostranstve: ratione materiae, ratione temporis i problema kvalifikatsii kiberatak [International Humanitarian Law in Cyberspace: Ratione Materiae, Ratione Temporis and Problem of Cyber-Attack Qualification]. Tsifrovoe pravo, vol. 2, no. 1, pp. 64–80. (In Russian).

Garkusha-Bozhko S. Yu. (2023) Opredelenie vooruzhennogo konflikta v kiberprostranstve [The Definition of Armed Conflict in Cyberspace] // Vestnik of Saint Petersburg University. Law, vol. 14, no. 1, pp. 194–210. (In Russian).

Geiss R., Lahmann H. (2021) Protection of Data in Armed Conflict. International Law Studies, vol. 97, no. 556, pp. 556–572.

Faisal S., Emad A. A., Sultan I. A. (2022) International Responsibility Arising from Cyberattacks in the Light of Contemporary International Law. International Journal of Cyber Criminology, vol. 16, no. 1, pp. 156–169.

Ivanova K. A., Myltykbaev M. Zh., Shtodina D. D. (2022) Ponyatie kiberprostranstva v mezhdunarodnom prave [The Concept of Cyberspace in International Law]. Pravoprimenenie, vol. 6, no. 4, pp. 32–44. (In Russian).

Kapustin A. Ya. (2022) Suverenitet gosudarstva v kiberprostranstve: mezhdunarodno-pravovoe izmerenie [Sovereignty in Cyberspace: International Legal Dimension]. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'noogo pravovedeniya, vol. 18, no. 6, pp. 99–108.

Laurent G., Tilman R., Knut D. (2020) 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, pp. 287–334.

Mačák K. (2015) Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law. Israel Law Review, vol. 48, no. 1, pp. 55–80.

Mačák K. (2021) Unblurring the Lines: Military Cyber Operations and International Law. Journal of Cyber Policy, vol. 6, no. 3, pp. 411–428.

Manevich V. V. (2024) Mezhdunarodno-pravovoe regulirovanie primeneniya kibersredstv pri vedenii vooruzhennykh konfliktov: pravovye osnovy i nauchnye discussii [International Legal Regulation of the Use of Cyber Means in Armed Conflicts: Legal Foundations and Scientific Discussions]. Zakon i Pravo, vol. 12, no. 2, pp. 275–282. (In Russian).

McCormack T. (2018) International Humanitarian Law and the Targeting of Data. International Law Studies, vol. 94, no. 1, pp. 222–240.

Ottis R. (2008) Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare perspective. 7th European Conference on Information Warfare and Security 2008, pp. 163–168.

Pomson O. (2023) ‘Objects’? The Legal Status of Computer Data under International Humanitarian Law. Journal of Conflict and Security Law, vol. 28, no. 2, pp. 349–387.

Roscini M. (2014) Cyber Operations and the Use of Force in International Law, Oxford: Oxford University Press.

Rusinova V. N. (2018) Mezhdunarodno-pravovoy printsip nevmeshatel’stva i kiberoperatsii: neopravdannye ozhidaniya? [The International Legal Principle of Non-interference and Cyber-operations: Unjustified Expectations?]. Mezhdunarodnoe pravosudie, no. 1, pp. 38–52. (In Russian).

Rusinova V. N. (2022) Mezhdunarodno-pravovaya kvalifikatsiya vredonosnogo ispol’zovaniya informatsionno-kommunikatsionnaykh technologii: v poiskakh konsesusa [Qualification of Harmful Use of Information and Communications Technologies Under International Law: In Search of a Consensus]. Moscow Journal of International Law, no. 1, pp. 38–51. (In Russian).

Schmitt M. N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press.

Schmitt M. N. (2017) Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, 2nd ed., Cambridge: Cambridge University Press.

Schmitt M. N. (2019) Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations. International Review of the Red Cross, vol. 101, no. 910, pp. 333–355.

Schondorf R. (2021) Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. International Law Studies, vol. 97, no. 395, pp. 395–406.

Spaic B. (2023) Evolutionary and Static Interpretation. In: Załuski W. (ed.) Research Handbook on Legal Evolution, Edward Elgar Publishing.

Veljković S. (2024) Possibility of Applying the Rules of International Humanitarian Law to Cyber Warfare. Pravo – Teorija I Praksa, vol. 41, no. 3, pp. 17–28.

Vöneky S. (2008) Analogy in International Law. In: Wolfrum R. (ed.) Max Planck Encyclopedia of Public International Law, Oxford: Oxford University Press.