Reviw Article
DOI: https://doi.org/10.22598/iele.2025.12.1.12

INTERNATIONAL ARMED CONFLICTS IN CYBERSPACE [*]

Bence Kis Kelemen [**]

ABSTRACT

States employ their cyber capabilities to replace, support or complement their traditional kinetic operations. When it comes to replacing physical violence altogether, the question arises, whether cyber operations in and of themselves are capable of triggering the application of international humanitarian law in the context of an international armed conflict. Analysis of the applicable law shows that an armed conflict exists whenever there is recourse to armed force, which ultimately boils down the attacks under international humanitarian law. If a cyber operation constitutes an attack, then it is capable of triggering the application of an international armed conflict. This usually requires death or injury to persons and damage or destruction to objects. There is however a wide disagreement in literature and in state practice as to what exactly constitutes an attack in the cyber domain. This article argues that state practice (accepted as law) is inconclusive to suggest, that cyber operations causing loss of functionality or deletion of electronic data without physical damage would also trigger an armed conflict between states, despite the undeniable trend in both state practice and scholarly writings to the contrary.

Keys words: *international humanitarian law, attack, cyber operations, cyber attacks, armed conflict.*

1. INTRODUCTION

The Russo-Ukrainian armed conflict, that has dominated the headlines in the past 3 years, primarily takes place in the physical realm. Tanks, combat aircraft, armoured vehicles, and, of course, fighters from both sides play the

[**] The article is based and developed further on a similar article of the author published in Hungarian: Kis Kelemen, B.: Nemzetközi fegyveres konfliktusok a kibertérben, *Közjogi Szemle*, (3) 2023, pp. 39-47.

[*] University of Pécs, Faculty of Law, Pécs, Hungary, kis.kelemen.bence@ajk.pte.hu

leading roles in this confrontation. However, it is important to note that beneath the surface, another conflict is unfolding—in cyberspace. One significant player in this arena is the IT Army of Ukraine, a non-state actor that operates through Ukrainian and international volunteer hackers in collaboration with the Ukrainian Ministry of Defence to target Russian entities.[1] The organization regularly shares its achievements through its X (Twitter) channel.[2] Another organization of note is the Cyber Partisans of Belarus., that also participates in the conflict on the side of Ukraine.[3] Alongside Ukraine, the Russian side is also active in cyberspace, for instance, through the Killnet or the Cyber Army of Russia.[4] It is worth mentioning, though, that contrary to expectations, the Russian Federation hasn't been particularly successful in their cyberspace combat against Ukraine.[5]

Both in the present and the past, states have employed cyber attacks to support their conventional military operations. For example, in 2007 Israel hacked into the Syrian air defence system to successfully bomb an alleged nuclear plant.[6] Cyber operations usually aim for substituting, supporting or complementing kinetic operations.[7] In the literature, it appears indisputable that such cyber operations must comply with international law, particularly the rules of international humanitarian law (IHL). The second edition of the Tallinn Manual, which is considered a private codification effort or in other words a non-binding scholarly work,[8] stipulates in Rule 80 that cyber operations con-

1 <https://www.cfr.org/cyber-operations/ukrainian-it-army>.

2 <https://twitter.com/ITArmyUKR>.

3 Biggio, G., The Legal Status and Targetability of Hacker Groups in the Russia-Ukraine Cyber Conflict, *Journal of International Humanitarian Legal Studies*, 15(1) 2024, pp. 146-147.

4 <https://www.bbc.com/news/technology-65250356>.

5 <https://rusi.org/explore-our-research/publications/commentary/all-quiet-cyber-front-explaining-russias-limited-cyber-effects>.

6 Eilstrup-Sangiovanni, M.: Why the World Needs an International Cyberwar Convention, *Philosophy & Technology*, 31(3) 2018, p. 379.

7 Egloff, F. J., Shires, J.: Offensive Cyber Capacities and State Violence: Three Logics of Integration, *Journal of Global Security Studies*, 7(1) 2021, p. 3.

8 The book can be considered a form of private codification because the document represents the understanding of the expert team working on the first and second editions regarding international legal rules applicable in cyberspace. See Schmitt, M. N. (ed.): *Tallin Manual 2.0 On the International Law Applicable to Cyber Operations*, New York: Cambridge University Press, 2017. p. 2. Based on this, its authority falls far behind the documents prepared by the International Law Commission–an organization which plays a role in the traditional codification process and–to which customary legal force is generally attributed, albeit to varying degrees. The legal nature of rules produced in this context more closely resembles the legal binding force of a document created through an identification process. Therefore, the rules of

ducted within the context of armed conflicts fall within the scope of the law of armed conflict.[9]

However, the legal assessment of situations is doubtful where we cannot speak of a conventional armed conflict in the kinetic domain, yet two states use force against each other in cyberspace. This study seeks to provide clarity in this question by examining the conditions under which international armed conflicts (IACs) are created and whether those conditions can be met in case of a purely cyber armed conflict[10] (Section II). The article then provides an overview of the available and relevant state practice and *opinio juris* regarding what states consider as armed conflicts in the cyber context, both directly and indirectly (Section III). Finally, it draws its conclusions (Section IV), summarizing that international law does not exclude the possibility of a purely cyber armed conflict between states. However, there is a discrepancy regarding the threshold at which the rules of IHL become applicable to a particular operation or type of operation (the question of the *de minimis* threshold).[11] This article argues that state practice (accepted as law) at this point is inconclusive to suggest that cyber operations causing loss of functionality without physical damage would also trigger an armed conflict between states, despite the undeniable trend in both state practice and scholarly writings to the contrary.

2. INTERNATIONAL ARMED CONFLICTS IN CYBERSPACE

In this Section, the author examines the conditions under which an IAC is triggered, which would then make IHL applicable to the conflict in question. Subsequently, the author seeks to answer the question of which actions carried

the Tallinn Manual can only be accepted as reflecting customary law to the extent that they are accompanied by appropriate state practice and *opinio juris*. See International Court of Justice: *North Sea Continental Shelf, Judgment*, ICJ Reports 1969, p. 3, para. 77.

9 Schmitt, M. N., op. cit. (ref. 8.), p. 375.

10 Within the context of this article, a purely cyber confilict refers to armed confrontations where hostilites take place exclusively in the cyberspace, for example through launching a malware. This makes it possible to differentiate between armed conflicts with cyber elements, the latter which depicts traditional kinetic uses of force (e.g. launching airstrikes), mixed with cyber operations designed to support or supplement kinetic operations (e.g. shutting down the air defense system of the adversary moments before the airstrike).

11 It should be mentioned at the outset, that the vast majority of international legal scholars and international (criminal) tribunals maintined for long, that there is no intensity treshold for the application of IHL in IACs. It is curious that despite this, Section IV will explore a handful of statements from states arguing for the contrary. See: Grignon, J.: The Beginning of Application of International Humanitarian Law: A Discussion of a Few Challenges, *International Review of the Red Cross*, 96(893) 2014, pp. 152–153.

out in cyberspace bring about the application of the rules of IHL in inter-state cyber conflicts.

2.1. CONDITIONS PERTAINING TO THE DETERMINATION OF AN INTERNATIONAL ARMED CONFLICT

The definition of IACs must begin with the concept of armed conflicts. One of the perhaps most eloquent formulations of this concept comes from the International Criminal Tribunal for the former Yugoslavia (ICTY), which stated in its Tadić-decision 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. […]"[12]

Based on the above, two types of armed conflicts are recognized: inter-state, also known as international armed conflicts, and intra-state,[13] meaning non-international armed conflicts.[14] Considering that the focus of the study is on the applicability of cyber operations in inter-state contexts, further investigation will be limited to the realm of IACs.

In order to understand how modern international law regulates IACs and which situations qualify as such, it is useful to refer to Common Article 2 to the 1949 Geneva Conventions. The first paragraph of these Articles states that:n"[…] the present Convention 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."[15]

---

[12] See Case IT-94-1 Prosecutor v. Dusko Tadić, (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Appeals Chamber, 2 October 1995, para. 70.

[13] It is essential to note here that the phrase 'intra-state' does not imply that a non-international armed conflict can only take place within the territory of a single state or that it can only occur in the territory of the state that is confronted by certain non-state actors or organized armed groups. The determination of non-international armed conflicts is not hindered by the so-called 'spill-over effect', which occurs when an internal conflict extends to the territory of another state. See Kis Kelemen, B.: *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására*, Pécs: Publikon Kiado, 2023, pp. 152-153. We have observed such conflicts on numerous occasions in the past two decades in the Middle East, for example, when the Islamic State extended its activities from Iraq to Syria in 2013. <https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state>.

[14] Dinstein, Y.: *War, Agression and Self-Defence*, 5th edition, Cambridge: Cambridge University Press, 2011, pp. 5-6.

[15] Geneva Convention relative to the Protection of Civilian Persons in Time of War, 12 August 1949, art. 2.

According to these principles, IHL must be applied when parties declare war on each other or become engaged in any other armed confrontation. This is regardless of whether the parties recognize the existence of the conflict or not. A good example of the latter situation is once again provided by the Russo-Ukrainian armed conflict, in which Russia referred to its invasion against Ukraine in 2022 as 'special military operations'.[16] As for the significance of a declaration of war, Oppenheim already stated at the beginning of the 20th century that sending such a declaration is not a mandatory rule of general international law. The absence of a declaration of war or ultimatum does not affect the development of a state of war between the parties.[17]

The 1952 commentary on the First Geneva Convention from 1949 (GCI),[18] prepared by Jean Pictet, highlights that the use of the term 'armed conflict' in the treaty was not accidental. Its purpose was to make it difficult for states to consider the provisions of the treaty inapplicable on various grounds, as they had previously done when the applicable law regulated 'war'.[19] The 1952 commentary defines the concept of armed conflict as "[a]ny difference arising between two States and leading to the intervention of armed forces […]".[20] According to Pictet, the duration of the conflict or the extent of the slaughter is irrelevant. Thus, even the injury of a single person can be sufficient to establish an armed conflict.[21] However, the 2016 commentary issued by the International Committee of the Red Cross (ICRC) goes further than the 1952 formulation of 'intervention of armed forces' and aligns itself with the Tadić-decision, defining armed conflict as hostile resort to armed force by one or more states against another.[22] The 2016 commentary also emphasizes that

16 United Nations Security Council: *Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*, New York: United Nations, 24 February 2022, p. 6. It should be noted that the use of the term was likely based on internal legal reasons, possibly related to Russian law. See Hoffmann, T.: War or peace? - International legal issues concerning the use of force in the Russia-Ukraine conflict, *Hungarian Journal of Legal Studies*, 63(3) 2022, p. 208.

17 Oppenheim, L.: *International Law a Treatise*, 2nd edition, London: Longmas Green, 1926, p. 193 & p. 199.

18 ICRC: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), Geneva: ICRC, 1949.

19 Pictet, J.: *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field,* Geneva: ICRC, 1952, p. 32.

20 Ibid.

21 Ibid.

22 International Committee of the Red Cross: *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, Cambridge: Cambridge University Press, 2016, paras. 218-219.

the Pictet commentary's formulation of the 'intervention of armed forces' is too narrow since it excludes cases where only one party employs unilateral force against another state. However, these cases are clearly within the scope of IHL.[23] Another important observation is that the applicability of the law of armed conflicts is not conditional on the use of armed force against enemy armed forces. IHL is applicable even when violence is directed at the territory, civilian population, or civilian objects, including civil infrastructure, of another state.[24] In terms of the use of force, the emphasis is on attribution[25] to the state rather than on the status of the perpetrator, *i.e.* state's armed forces.[26] Finally, and most importantly, in the context of international armed conflicts, unlike non-international armed conflicts,[27] there is no concept of an intensity threshold. Even minor clashes, provided they are not accidental or *ultra vires*, can trigger the application of international humanitarian law.[28]

The First Additional Protocol from 1977 (API) to the 1949 Geneva Conventions similarly addresses this issue. Article 1(3) of API refers back to Common Article 2 to the 1949 Geneva Conventions, which is further supplemented by Article 4, applying the law of international armed conflicts to the right to self-determination, colonial domination, foreign occupation, and struggles against racist regimes.[29] The 1987 commentary to API essentially repeats the original Pictet commentary.[30]

---

[23] Ibid., paras. 221-223.

[24] Ibid., para. 224.

[25] On attribution in international humanitarian law. See Kajtár, G.: *Betudás a nemzetközi jogban. A másodlagos normák szerepe a beruházásvédelemtől a humanitárius jogig*, Budapest: ORAC, 2022. pp. 57-76.

[26] International Committee of the Red Cross, op. cit. (ref. 20), paras. 225-229.

[27] The intensity threshold is reached in those conflicts where the state needs to take armed and military action against an organized armed group. See Weizmann, N.: Armed Drones and the Law of Armed Conflict, in: Casey-Maslen, S., Homayounnejad, M., Stauffer, H., Weizmann, N. (eds.): *Drones and Other Unmanned Weapons Systems under International Law* (pp. 89-122), Leiden: KONINKLIJKE BRILL NV, 2018, p. 94.

[28] International Committee of the Red Cross, op. cit. (ref. 22), paras. 236-237 and para. 241.

[29] International Committee of the Red Cross: *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 8 June 1977*, Geneva: International Committee of the Red cross, May 2010, art 1. paras 3-4. (hereinafter: AP I).

[30] Sandoz, Y., Swinarski, C., Zimmermann, B. (eds.): *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva: Oxford University Press, 1987, pp. 39-40, paras. 57-63.

Based on the above, it can be concluded that IACs, and thus the applicability of IHL, can be identified when a state's attributable conduct involves intentional and hostile use of armed force against another state.

However, at this point, it is necessary to briefly distinguish the concept of 'use of armed force' for the purposes of the law of armed conflicts from the concept of 'armed attack'[31] or the use of (armed) force applicable in the context of *jus ad bellum*.[32] It should be noted that these terms do not necessarily have the same meaning in IHL and *jus contra bellum*. These two branches of law deal with fundamentally different issues and have different rules. While the former primarily establishes rules for the parties involved in armed conflicts, the latter prohibits cross-border uses of force and regulates the limited exceptions where such uses of force may be justified. However, this does not exclude the possibility that a specific conduct simultaneously constitutes a prohibited (armed) use of force in the context of *jus ad bellum* and invokes the law of armed conflicts. For example, a targeted killing operation carried out between states fulfils both criteria simultaneously.[33]

Having considered the above, let us return to our original line of argument and examine which specific behaviours can qualify as intentional and hostile use of armed force from the perspective of IHL. In this regard, the 2016 commentary is helpful, as it states that: "[…] any attack directed against the territory, population, or the military or civilian infrastructure constitutes a resort to armed force against the State to which this territory, population or infrastructure belongs."[34]

---

[31] Charter of the United Nations, Art. 51. International Court of Justice: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, p. 14. para. 191.

[32] Charter of the United Nations, Art. 2. para. 4. See While the UN Charter only refers to the use of force and the threat thereof, scholarship defines the use of force as armed force/violence. Casey-Maslen, S.: *Jus ad Bellum – The Law on Inter-State Use of Force*, Oxford: Hart Publishing, 2020, p. 22.

[33] However, it should be emphasized that these two systems are independent of each other, meaning that something can be unlawful under *jus contra bellum* and lawful under the law of armed conflict at the same time. Of course, the reverse is also true. See Stahn, C.: 'Jus ad bellum', 'jus in bello' ... 'jus post bellum'? – Rethinking the Conception of the Law of Armed Force, *European Journal of International Law*, 17(5) 2006, pp. 924-925. The distinction between these two areas is important because in the literature, we often come across confusions or mix-ups between the different notions. For example, Phillip McReynolds confuses the concept of attack in IHL with the category of armed attack in *jus ad bellum*. See McReynolds, P.: How to Think About Cyber Conflicts Involving Non-state actors, *Philosophy & Technology,* 28(3) 2015, p. 432.

[34] International Committee of the Red Cross, op. cit. (22), para. 224.

Indeed, this means that the concept of 'attack' in the law of armed conflicts is synonymous with the resort to armed force, and therefore, with the existence of IACs. Consequently, I will now focus on the concept of 'attack' as an institution within IHL.

2.2. ATTACK IN THE LAW OF ARMED CONFLICTS

The concept of 'attack' is defined in API, which states that an attack refers to acts of violence against the enemy, whether of offensive or of defensive nature.[35] The 1987 commentary takes a position on this matter, stating that an attack must involve some form of combat action.[36] Yoram Dinstein highlighted that non-violent conduct, such as interrupting enemy communication or engaging in psychological warfare, does not fall within the concept of attack.[37] Anne Quintin argues that acts of force must reduce the enemy's military capabilities and potential, therefore, operations that destroy, damage, or neutralize enemy targets fall under the category of attack.[38] This connects the concept of attack to the notion of military objectives and civilian objects within international humanitarian law.[39]

2.3. CAN CYBER OPERATIONS QUALIFY AS ATTACKS?

First, it must be stated that the international community is in consensus that the rules of international law are applicable in cyberspace.[40] However, there is a lack of consensus regarding the applicability of IHL in cyberspace[41] and, if applicable, in what form.[42] The first problem can be resolved relatively simply

[35] AP I, op. cit. (ref. 29), Art 49. para. 1

[36] Sandoz, Y., Swinarski, C., Zimmermann, B., op. cit. (ref. 30), para. 1880.

[37] Dinstein Y.: *The Conduct of Hositilities under the Law of International Armed Conflict,* 3rd edn, Cambridge: Cambridge University Press, 2016, p. 3.

[38] Quintin, A.: Attacks, in: Djukić, D., Pons N. (eds.): *The Companion to International Humanitarian Law*, Leiden: BRILL, 2018, p. 191.

[39] AP I, op. cit. (ref. 29), Art. 51. para. 2. and Art. 52. paras. 1-2

[40] International Committee of the Red Cross: *International humanitarian law and the challenges of contemporary armed conflicts report*, Geneva: International Committee of the Red Cross, 32IC/15/11, October 2015, p. 39.

[41] Mačák, K.: 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, p. 3.

[42] See *e.g.* the difference of opinion on the object status of electronic personal data. See Kis Kelemen, B.: Protection of (Personal) Data in Armed Conflicts, *Baltic Journal of Law & Pol-*

by referring to the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons. In their decision, the Hague judges stated that although the invention of nuclear weapons occurred after the development of the principles of IHL, their application to these weapons cannot be denied based on this fact. To deny their application would contradict the humanitarian nature of the legal framework, so the law must be applied to past, present, and future weapons in the same manner.[43] Considering that cyber warfare, including cyber attacks, is similar to nuclear weapons in the sense that their invention followed the development of principles of IHL, we can likely draw the same conclusion regarding the application of this legal framework to these military operations. Furthermore, countries such as Russia and China may not consider the law of armed conflict applicable in cyberspace because they view it as something that is legitimizing war and military operations in this context.[44] However, in agreement with Kubo Mačák's position, such opinions cannot be sustained because the fact that the law regulates a particular behaviour does not necessarily mean it legitimizes it at the same time. On the contrary, IHL seeks to limit the conduct of parties engaged in armed conflicts.[45] Based on the above, it must be firmly established that international law, including the law of armed conflicts, is applicable in cyberspace. This assertion is reinforced by Rule 80 of the Tallinn Manual, which was also referenced in the introduction.[46]

Returning to the objective of this study, it is necessary to examine whether a cyber operation alone can give rise to an armed conflict, specifically an IAC, or in other words, whether a cyber attack alone can meet the threshold for the applicability of international humanitarian law. The Tallinn Manual suggests that such a situation is not excluded, as Rule 82 states, "[a]n international armed conflict exists whenever there are hostilities, which may include or be

itics, 17(1) 2024, pp. 4-9. Furthermore, Israel has raised the existence of domain specific rules. See Akende, D., Coco, C., de Souza Dias, T.: Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies, *International Law Studies*, 99(1) 2022, p. 8. This argument has however been disproved. See Akende, D., Coco, C., de Souza Dias, T., op. cit. (ref. 42), p. 12.

43 International Court of Justice: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, *ICJ Reports*, 1996, p. 226. para. 86.

44 <https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>. In the case of Russia and China, see Akende, D., Coco, C., de Souza Dias, T., op. cit. (ref. 42), pp. 6-7. Cuba is also mentioned in the source, however this position has changed in 2024, see Section III.

45 Mačák, K., op. cit. (ref. 41), para. 3.

46 Schmitt, M. N., op. cit. (ref. 8), p. 375.

limited to cyber operations, between two or more states."[47] (Emphasis added) The accompanying commentary to the rule unambiguously states that cyber operations alone are capable of constituting hostilities and thereby establishing an armed conflict.[48] This rule and its commentary indicate that the majority of international legal experts, without dissent in this case, believe that cyber operations alone can give rise to an international armed conflict. The 2016 commentary on the GCI also states that certain cyber operations, particularly those with similar consequences to classical kinetic operations, are capable of creating an IAC.[49] Laurie R. Blank shares this view, stating that such armed conflicts are likely to be short in duration and limited in scope.[50] However, Kriangsak Kittichaisaree is unsure whether a cyber attack alone is capable of triggering an armed conflict.[51]

Nevertheless, there was disagreement among the experts involved in the creation of the Tallinn Manual regarding whether a particular individual cyber operation can trigger the law of armed conflicts, which was unclear even in the notorious 2010 Stuxnet[52] case.[53] Similar doubts arose in the aforementioned 2016 commentary as well.[54]

Based on the above, it is evident that cyber operations can indeed lead to an IAC, but it is necessary to determine which cyber operations are capable of doing so. The remaining part of this study will address this question.

47 Schmitt, M. N., op. cit. (ref. 8), p. 379.

48 Schmitt, M. N., op. cit. (ref. 8), p. 383.

49 International Committee of the Red Cross, op. cit. (ref. 22), para. 255.

50 Blank, L. R.: Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace, in: Ohlin, JD., Govern, K., Finkelstein, C. (eds.): *Cyberwar. Law and Ethics for Virtual Conflicts*, Oxford: Oxford Academic, 2015, pp. 81-82. The author argues, however, that a purely cyber conflict is unlikely, contrasting it with the rhetoric of 'cyberwar', which is seen as problematic when compared to the fight against terrorism. See Blank, L R., op. cit. (ref. 50), p. 85 and 88.

51 Kittichaisaree, K.: *Public International Law of Cyberspace*, Cham: Springer, 2017, p. 204.

52 Stuxnet was a malicious worm developed alegedly through Israeli-American cooperation that targeted the Iranian nuclear program by destroying centrifuges used for uranium enrichment. The case is significant in that the said malware spread to other computers as well, although it did not cause any damage outside of of the Iranian nuclear program. <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>.

53 Schmitt, M. N., op. cit. (ref. 8), pp. 383-384.

54 International Committee of the Red Cross, op. cit. (ref. 22), para. 256.

2.4. ATTACKS IN CYBERSPACE

Summarizing the findings so far, it can be determined, that the existence of IACs requires the resort to armed force. This armed force can occur exclusively in cyberspace as well. According to the rules of IHL, the use of armed force can be unequivocally determined, when the same conduct constitutes an attack as well. Therefore, the last two determinations that need to be made are: *1)* which operations qualify as an attack and *2)* whether the term 'cyber attack' is applicable or preferable for describing this phenomenon.

According to API and legal doctrine, an attack in the context of the law of armed conflict occurs when violent actions of an offensive or defensive nature are carried out.[55] This means that we must look for cyber operations that meet the aforementioned criterion. The Tallinn Manual defines a cyber operation as the "employment of cyber capabilities to achieve objectives in or through cyberspace."[56] This is part of the broader concept of cyber activity, which refers to the use of cyber infrastructure or other cyber means to influence such infrastructure.[57] The term 'cyber' itself derives from the Greek word '*kybernetes*,' meaning governance or control, and refers to the science of remote control through devices.[58]

Dinstein argued that a cyber attack qualifies as an attack when it results in the death or injury of human beings, or the destruction or damage of objects. According to him, breaching a firewall or installing malware does not qualify as an attack. However, the shutdown of a life-sustaining program or causing a devastating fire in an electrical grid is considered an attack.[59] Not surprisingly, the Oslo Manual on Select Topics of the Law of Armed Conflict, edited by Dinstein and Arne Willy Dahl also argued that physical damage is necessary for an attack to take place, and loss of functionality is generally not regarded as enough for an operation to constitute an attack.[60] Elaine Korzak and James Gow share the same view, arguing that the determination of whether a cyber operation qualifies as an attack should be made on a case-by-case basis, con-

[55] See Section II, point 2.

[56] Schmitt, M. N., op. cit. (ref. 8), p. 564.

[57] Ibid.

[58] Akende, D., Coco, C., de Souza Dias, T., op. cit. (ref. 42), pp. 19-20.

[59] Dinstein, Y., op. cit. (ref. 37), pp. 2-3. Regarding the installation of a malware, it should be noted that in my opinion, the installation of malware that causes damage over a delayed period of time, as described above, can also be considered an attack, similar to how we view the installation of landmines as an attack. See Quintin, A., op. cit. (ref. 38), p. 193.

[60] Dinstein, Y., Dahl, A. W.: O*slo Manual on Select Topics of the Law of Armed Conflict. Rules and Commentary*, Cham: Springer, 2020, p. 22.

sidering its consequences.[61] On the other hand, Marco Roscini introduces an interesting perspective. He initially states that the destruction of a computer alone is not capable of creating an armed conflict, but the greater the damage, the more likely it is, that such a conflict exists.[62] In this regard, the author introduces an intensity threshold for cyber conflicts. He then asserts that the deletion, alteration, or corruption of electronic data does not constitute an attack but is part of hostilities.[63] Furthermore, he suggests that functional damage, *i.e.* the non-functionality of infrastructure as a consequence, is a requirement for determining an attack, using the analogy of a graphite bomb. However, he also states that the attacker cannot necessarily know in advance whether the attack can be remedied by replacing a physical component, such as hardware, or by software replacement such as reinstallation.[64] In my opinion, the first and second statements on operations against data are not compatible with each other, as software replacement essentially affects the data stored on the hardware. If functionality can be restored in this way, then the attack affected the data, and thus, the two statements cannot be simultaneously upheld. Cordula Droege highlights the temporary nature of functionality loss, which does not necessarily need to be permanent.[65] Blank also holds the view that the consequences of a military operation determine whether it qualifies as an attack, referring to biological, chemical, and radiological weapons.[66] The author argues that there is a *de minimis* threshold, meaning insignificant consequences do not establish an attack.[67] It should be noted that there is a debate regarding which

[61] Korzak, E., Gow, J.: Computer network attacks under the jus ad bellum and the jus in bello. 'Armed' – effects and consequences', in: Gow, J., Dijxhoorn, E., Kerr, R., Verdirame, G. (eds.): *Routledge Handbook of War, Law and Technology*, New York: Routledge, 2021, pp. 71-73. However, it is worth noting that the author duo seemingly confuses the issues of *jus in bello* and *jus ad bellum*, which can be excused to some extent, as a *jus contra bellum*, use of force, can also be considered an 'attack' from an IHL perspective. However, it is important to separately discuss these questions due to the different tests involved. Additionally, it should be mentioned that the issue of armed attack and the use of force also revolves around its consequences and effects in *jus ad bellum* as well. See Schmitt, M. N., op. cit. (ref. 8), p. 330.

[62] Roscini, M.: *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014, p. 135.

[63] Ibid., pp. 178-179.

[64] Ibid., pp. 180-181.

[65] Droege, C.: Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians, *International Review of the Red Cross*, 94(886) 2012, p. 559.

[66] Blank, L. R., op. cit. (ref. 50), p. 93.

[67] Ibid. The problem arises here that states do not classify every clash between them as an armed conflict. The root cause behind this are usually political reasons rather than an *opinio juris* that the specific level of intensity does not reach the required threshold. See Arimatsu, L.: Classifying cyber warfare, in: Tsagourias, N., Buchan R. (eds.): *Research Handbook on*

operations are subject to the principles of IHL. Blank, for example, argues that these principles apply only to attacks.[68] However, Géza Herczegh, who participated in the codification process of API, emphasized in his monograph that the principle of distinction applies to all military operations.[69] This study does not aim to take a position in this debate. Nevertheless, it is worth mentioning that, in the author's opinion, some principles of IHL, if not all, could be applicable in the broader context of military operations, not exclusively in relation to attacks. Rule 92 of the Tallinn Manual determines the concept of cyber attack in a similar manner. Accordingly, a cyber attack is defined as any offensive or defensive cyber operation that reasonably results in the injury or death of persons or the destruction or damage of objects.[70] Therefore, it is possible to launch an attack against computer data if it leads to the above-mentioned outcomes.[71] The majority of experts involved in the creation of the Tallinn Manual believed that the functionality of assets being compromised also qualifies as an attack since it ultimately entails harm or destruction. For some experts, this meant replacing physical components, while for others, it involved modifying data, such as reinstalling software. Some experts argued that the manner in which functionality is lost is irrelevant.[72] On the contrary, Ori Pomson holds the view that some form of physical damage is necessary to establish an attack. The author illustrates this argument with the vivid example that in the absence of the requirement of physical harm, even scrolling through a text document could be considered an attack, since it also changes the electronic data of the text document, specifically the binary signals that constitute the file.[73] It is appropriate to pause here and refer to the problem related to the status of electronic data as objects of military objectives. If we accept the definitions of attack presented above, it can be concluded that an attack occurs when a person dies or is injured, or when an object (civilian objects or military objectives) is destroyed or damaged. However, if electronic data were considered an object, the category of attack within the framework of IHL would significantly expand, as it would encompass not only the destruction and damage of tangible objects in physical

International Law and Cyberspace (pp. 406-426), Northampton: Edward Elgar Publishing Inc., 2021, pp. 414-415.

68 Blank, L. R., op. cit. (ref. 50), p. 92.

69 Herczegh, G.: *A humanitárius nemzetközi jog fejlődése és mai problémái*, Budapest: Közgazdaság lap- és könyvkiadó, 1981, pp. 196-198.

70 Schmitt, M. N., op. cit. (ref. 8), p. 415.

71 Schmitt, M. N., op. cit. (ref. 8), p. 416.

72 Schmitt, M. N., op. cit. (ref. 8), pp. 417-418.

73 Pomson, O.: 'Objects'? The Legal Status of Computer Data under International Humanitarian Law, *Journal of Conflict & Security Law*, 28(2) 2023, pp. 352-354.

space but also the modification and deletion of electronic data, without the necessity to include physical harm as a consequence of deleting or manipulating with computer data. This study does not aim to extensively examine this issue, but it is important to note that there is a trend in scholarship and state practice that is starting to accept the status of electronic data as objects, although current law and state practice do not yet support this.[74]

In summary, the literature appears to be unanimous in stating that an attack occurs when someone is killed or injured, or when an object is destroyed or damaged as a result of a military operation. Some argue that the latter category can also involve the impairment of functionality. Therefore, a cyber operation can be considered an attack if at least one of the aforementioned outcomes is realized. This inherently excludes cyber espionage[75] and a significant portion of attacks involving denial of service (DoS) from the scope of attacks, even though they may have significant adverse effects on the civilian population.[76]

Finally, it is necessary to address whether the term 'cyber attack' is preferable or even accurate for describing attacks within the context of IHL. In the author's opinion, the answer is clearly no. In many cases, the term 'cyber attack' is used differently[77] from the aforementioned context, encompassing a large number of cyber operations. Therefore, agreeing with Blank,[78] it would be more appropriate to use the term "cyber operation" to describe the cyber nature of the operation and introduce the concept of "attack in cyberspace" for describing attacks within the framework of the law of armed conflict happening within the confines of this new domain.

[74] Ibid., p. 386; Kis Kelemen, B., op. cit. (ref. 42), pp. 13-15. Marc Schack and Katrine Lund-Hansen for example advocate for a contextual interpretation of international law in this situation, resulting in the object status of data, if attacking it would cause more than mere inconvenience. Schack, M., Lund-Hansen, K., Attacking Data: Moving beyond the Interpretative Quagmire of the 'Data as an object', *Nordic Journal of International Law*, 92(3) 2023, pp. 364-365 & pp. 368-370.

[75] Schmitt, M. N., op. cit. (ref. 8), p. 415.

[76] Yoo, C. S.: Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures, in: Ohlin, JD., Govern, K., Finkelstein, C. (eds.): *Cyberwar. Law and Ethics for Virtual Conflicts* (pp. 175-194), Oxford: Oxford Academic, 2015, p. 186; Schmitt, M. N., op. cit. (ref. 8), p. 418.

[77] See *e.g.* <https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html> or <https://www.bbc.com/news/uk-wales-62442127>.

[78] Blank, L. R., op. cit. (ref. 50), p. 94.

3. STATE PRACTICE IN CYBERSPACE

Examining IACs occurring in cyberspace cannot be complete solely by reviewing the relevant scholarship, as the Statute of the International Court of Justice also emphasizes that the teachings of the most highly qualified publicists of various nations can only serve as subsidiary means for the determination of international law.[79] However, in order to determine what exactly constitutes the *lex lata* in terms of treaty and customary law, it will be the state practice accepted as law that provides the answer.[80] I subscribe to the views of Ori Pomson, claiming that customary international law cannot be interpreted, rather one needs to identify customary rules based on relevant practice and *opinio juris*.[81]

It is important to note that the presentation of state practice regarding the applicable international legal norms in cyberspace can be identified through states' issued statements and regional consultations organized primarily by the ICRC. In the author's opinion, these statements - at least the specific issued statements - also reflect the practice and *opinio juris* of states.

Considering that, based on Section II, the existence of an IAC fundamentally depends on whether a military operation that can be characterized as an attack takes place, the assessment of state practice also reflects this issue. Therefore, it is necessary to examine the relevant practice and legal convictions regarding the applicability of attacks in cyberspace. The summary and categorization of state practice are illustrated in Table 1. States appearing in this analsysis is an exhaustive list of states that have given a statement on international law applicable in cyberspace.

[79] Charter of the United Nations; International Court of Justice: Statute of the International Court of Justice, Art 38. (1) d).

[80] This view is also reinforced by the ICRC. See ICRC: International Humanitarian Law and the challenges of contemporary armed conflicts. 31st International Conference of Red Cross and Red Crescent, 2011, 31IC/11/5.1.2, p. 37.

[81] Pomson, O.: Methodology of identifying customary international law to cyber activities, *Leiden Journal of International Law*, 36(4) 2023, p. 1031.

Table 1. State practice on the notion of attacks in cyberspace

Loss of functionality on its own	Loss of functionality even if reinstallation can restore functionality
Japan (2021)[82], Italy (2021)[83], Canada (2022)[84], Ireland (2023)[85], Austria (2024)[86]	France (2019)[87], Germany (2021),[88] Romania (2021)[89], Finland (2020)[90], Norway (2021)[91], Costa Rica (2023)[92], Colombia (2025)[93]

[82] The statement does not specifically highlight the loss of functionality in connection with the concept of attack, but it considers such operations of this nature as unlawful. The footnote attached to the text refers to Article 12 of AP I, which prohibits attacks on medical units. <https://www.mofa.go.jp/files/100200935.pdf>.

[83] According to the Italian statement, operations that exceed a *de minimis* threshold and result in physical damage, death, injury, or disruption of critical infrastructure can be considered as attacks. <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>.

[84] Similarly to Italy, Canada also applies a *de minimis* threshold and asserts that damages caused to systems based on cyber infrastructure can be considered as attacks. Considering that the impairment of such systems does not necessarily entail the destruction of infrastructure, the loss of functionality as a possible consequence of an attack can be identified in case of Canada. <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a14>.

[85] Ireland subscribes to the view, that the loss of functionality is enough of a consequence to consider an operation as an attack, explaining „[t]o interpret the term otherwise would mean that a cyber-operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting civilians and civilian objects and would not be consistent with the object and purpose of the Geneva Conventions and their Additional Protocols." <https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf>.

[86] Austria claims that disabling an information and communications technology network would constitute an attack. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf>.

[87] France considers any loss of functionality as an attack when the affected state must take active measures to repair the infrastructure or system, such as repairing or replacing a component or reinstalling a network. <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>. Thus France regards any operation against the availability, integrity and confidentiality of data as an attack. See Ibid.

[88] Germany considers any operation that adversely affects communication, information, or other electronic systems, as well as the information itself, to be an attack. This does not preclude operations that have physical effects on objects and individuals to be seen as attacks. <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>.

[89] Romania considers data to be objects. See United Nations General Assembly: *Official compendium of voluntary national contributions on the subject of how international law*

	Romania (2021),[94] Finland (2020),[95] Norway (2021),[96] Costa Rica (2023),[97] Colombia (2025)[98]
Loss of functionality with the necessity the replace a physical component	**Same effects as kinetic attacks**
New Zealand (2020),[99] Israel (2020)[100]	Australia (2020),[101] Switzerland (2021),[102] Sweden (2022),[103] United Kingdom (2021),[104] Singapore (2021),[105] United States (2021)[106] Denmark (2023)[107] Czechia (2024)[108]
Given a statement regarding international law applicable in cyberspace, but did not refer to this question	**Incompatible position with international humanitarian law**

applies 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 resolution 73/266, United Nations General Assembly, 13.07.2021, A/76/136*, p. 78.

90 Finland considers data to be objects. See UNGA, International law and cyberspace. Finland's national positions: <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbb-de-623b-9f86-b254-07d5af3c6d85?t=1603097522727>; Letho, M.: Finland's views on International Law and Cyberspace, *Nordic Journal of International Law,* 92(3) 2023, p. 468.

91 Norway considers electronic data as objects; therefore the loss of functionality is considered an attack even in cases where only system reinstallation is required. See Manual of the Law of Armed Conflict, Norway, 2013, p. 210. This position is not affirmed in a 2023 position paper See Musæus, V.: Norway's Position Paper on International Law and Cyberspace, *Nordic Journal of International Law*, 92(3) 2023, p. 473.

92 Costa Rica specifically states that „the use of cyber operations by one State against another State, as long as those operations have effects comparable to classic kinetic operations" will constitute an international armed conflict. para. 42. However, Costa Rica also states that civilian data are objects. para. 50. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf>.

93 Colombia argues that the notion of attack needs to be further clarified in international law, however, „in terms of assessing a given "attack" in the context of cyberspace, Colombia currently identifies a cyber operation as an "attack" if it can be reasonably expected to cause injury or death to persons or damage or destruction to objects, including those causing loss of functionality without direct physical damage." Colombia further states, that civilian data is generally protected from direct cyber operations. See <https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf>, pp. 12-13.

94 Romania considers data to be objects. See UNGA. Official compendium of voluntary national contributions on the subject of how international law applies 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 resolution 73/266, 13 July 2021, A/76/136*, p. 78.

[95] Finland considers data to be objects. See UNGA, International law and cyberspace. Finland's national positions: <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727>; Letho, M.: Finland's views on International Law and Cyberspace, *Nordic Journal of International Law,* 92(3) 2023, p. 468.

[96] Norway considers electronic data as objects; therefore the loss of functionality is considered an attack even in cases where only system reinstallation is required. See Manual of the Law of Armed Conflict, Norway, 2013, p. 210. This position is not affirmed in a 2023 position paper See Musæus, V.: Norway's Position Paper on International Law and Cyberspace, *Nordic Journal of International Law*, 92(3) 2023, p. 473.

[97] Costa Rica specifically states that „the use of cyber operations by one State against another State, as long as those operations have effects comparable to classic kinetic operations" will constitute an international armed conflict. para. 42. However, Costa Rica also states that civilian data are objects. para. 50. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf>.

[98] Colombia argues that the notion of attack needs to be further clarified in international law, however, „in terms of assessing a given "attack" in the context of cyberspace, Colombia currently identifies a cyber operation as an "attack" if it can be reasonably expected to cause injury or death to persons or damage or destruction to objects, including those causing loss of functionality without direct physical damage." Colombia further states, that civilian data is generally protected from direct cyber operations. See <https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf>, pp. 12-13.

[99] According to New Zealand, the loss of functionality is included in the damage caused by an attack, which can be equivalent to the result of a kinetic attack. <https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf>.

[100] Israel also recognizes the existence of a *de minimis* rule, and the consequence of an attack must be death, injury, or physical damage. Therefore, the mere loss of functionality cannot be considered an attack unless it is caused by physical damage or if the loss of functionality is only part of the attack, which ultimately results in physical damage. See Schöndorf, R.: Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, *International Law Studies*, 97(1) 2021, pp. 400-401.

[101] Australia considers a cyber operation as an attack if it reaches the threshold level of kinetic attacks. <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>.

[102] Switzerland highlights that it is not yet clarified what exactly constitutes an attack in cyberspace. However, it can be considered as an attack if it directly or indirectly causes death, injury, destruction, or damage. The protection of data poses challenges in this regard. See 'Switzerland's position paper on the application of international law in cyberspace. <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf>.

[103] Sweden also emphasizes the effects of the operation but does not comment on the loss of functionality. <https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyber-

Brazil (2021),[109] Estonia (2021),[110] Iran (2020),[111] Kazakhstan (2021),[112] Kenya (2021)[113] The Netherlands (2021),[114] China (2021),[115] Russian Federation (2021)[116] African Union (2024)[117] Cuba (2024)[118]	Pakistan (2023)[119]

space.pdf>. It is worth noting that the statement directly refers to the Tallinn Manual. This position has been reinforced in a 2023 position paper, see Engdahl, O., Sweden's Position Paper on the Application of International Law in Cyberspace, *Nordic Journal of International Law,* 92(3) 2023, p. 496.

104 The United Kingdom associates the concept of an attack with effects that are identical or similar to kinetic operations. <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>.

105 Singapore does not explicitly address attacks, but it implies through the principle of proportionality that actions resulting in death, injury, or damage to property can be considered as attacks. See A/76/136*, op. cit. (ref. 89), p. 85.

106 Indirectly, the United States also highlights physical damage as the expected effect of an attack, and it also indicates with the phrase 'including shared physical infrastructure,' that a military operation beyond that might also be considered as an attack. See l. Koh, H. H.: International Law in Cyberspace. Remarks Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD. Sept. 18, 2012, *Harvard International Law Journal,* 54(1) 2012, p. 5.

107 Denmark also subscribes to the kinetic attack equivalency, adding that „[t]his definition also includes activity where substantial destruction is caused as a foreseeable secondary effect. For instance, if a military air traffic control system through a cyber operation is taken out of operation which causes foreseeable loss of human life or substantial damage to or destruction of physical objects." See Kjelgaard, J. M., Melgaard, U.: Denmark's Position Paper on the Application of International Law in Cyberspace, *Nordic Journal of International Law*, 92(3) 2023, p. 455.

108 <https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf>. This is a new development from earlier, when the state did not provide any position on this particular issue. <https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>.

109 According to Brazil, further analysis is required. See A/76/136*, op. cit. (ref. 89), p. 23.

110 A/76/136*, op. cit. (ref. 89), pp. 23-30.

111 <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>.

112 A/76/136*, op. cit. (ref. 89), pp. 51-52.

113 A/76/136*, op. cit. (ref. 89), pp. 52-54.

114 <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, and A/76/136*, op. cit. (ref. 89), p. 54-65.

The above table and categorization make it clear that state practice diverges regarding which cyber operations qualify as attacks from the perspective of the law of armed conflict. While a significant number of states agree with the functional approach outlined in the Tallinn Manual, there are still various sub-positions on this issue. Some states consider the re-creation of data (re-installation) is sufficient to determine an attack, while others insist on the replacement of physical components, and some do not specify the consequences of functionality loss.

However, it is also evident that a group of states takes the position that a cyber operation qualifies as an attack when its effects are equivalent to kinetic military operations. Upon closer examination, this category does not fundamentally differ from the case of functionality loss, specifically through repair by replacing physical components. In both cases, damage occurs to a physical object, requiring repair or replacement of a component to restore (full) functionality. Thus, there is no compulsory need to separate these two cases. An example of this is the so-called Chernobyl Virus, which was created in the 1990s with the aim of damaging the BIOS chip of computers, which could only be fixed by replacing the device.[120]

[115] <https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_People%27s_Republic_of_China_(2021)>

[116] A/76/136*, op. cit. (ref. 89), pp. 79-82.

[117] <https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y>.

[118] <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Documento_de_posici%C3%B3n_de_Cuba._Aplicaci%C3%B3n_del_Derecho_Internacional_a_las_TIC_en_el_ciberespacio..pdf>.

[119] Pakistan argues that IHL should prohibit cyber attacks that cause significant financial damage, undermine the confidentiality, integrity, and availability of critical civilian infrastructure, delete, destroy, or alter data necessary for the operation of critical civilian infrastructure, disrupt their functioning, or spread disinformation to create fear and chaos among the civilian population. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf>. It is generally accepted that operations that only cause inconvenience to the civilian population do not qualify as attacks. See Schmitt, MN., op. cit. (ref. 8), p. 418.

[120] <https://www.easytechjunkie.com/what-is-the-chernobyl-virus.htm>; <https://nakedsecurity.sophos.com/2011/04/26/memories-of-the-chernobyl-virus>.

In 2021, the ICRC organized two regional consultations jointly with other states and/or organizations to determine how the rules of IHL can be applied in cyberspace. In the consultation with Latin American states,[121] an agreement was reached that if the effects of a cyber operation are equivalent to those of a traditional kinetic operation, the law of armed conflicts can be applied.[122] However, there was disagreement regarding the extent of functionality loss that would lead to the determination of an attack.[123] The consultation with Central and Eastern European states[124] resulted in the understanding that attacks should be primarily judged based on their consequences, but there was no consensus on whether every instance of functionality loss constitutes an attack. While objections related to the functionality test were not raised, only a portion of the participants highlighted this issue on their own.[125]

Lastly, it is worth mentioning the position of the ICRC, although it is not a state. The ICRC emphasizes that operations causing death, injury, or physical damage should be considered attacks, and the result can occur directly or indirectly[126] (reverberating effects).[127] Additionally, the ICRC mentions that, in their view, functionality loss results in an attack even in the absence of physical damage.[128]

[121] The following states participated in the consultation: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Nicaragua, Paraguay, Peru, Uruguay. See International Committee of the Red Cross: *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, 27.12.2022, p. 15.

[122] Ibid., p. 6.

[123] Ibid., p. 7.

[124] The following states participated in the consultation: Czechia, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, and Slovenia. See International Committee of the Red Cross: *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, 27.12.2022, p. 11.

[125] Ibid., pp. 6-7.

[126] International Committee of the Red Cross: 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*, 102(913) 2020, p. 489. It should be emphasized, however, that this study does not address the discussion of the direct or indirect consequences of attacks.

[127] On reverberating effects see Kis Kelemen, B., op. cit. (ref. 13), pp. 165-166.

[128] ICRC, op. cit. (ref. 119), pp. 489-490.

These determinations mirror that of Ori Pomson, who claims that state positions are not representative of all geographical areas and disagreement among parties may preclude the emergence of a new customary international legal norm.[129]

4. CONCLUSION

Based on the above, it is useful to draw some key conclusions regarding IACs taking place in cyberspace. First and foremost, it should be emphasized that IHL is applicable to operations conducted in cyberspace, regardless of whether they involve kinetic operations or not. This means that cyber operations, in theory, have the potential to trigger an armed conflict between two or more states. Based on the study of international legal scholarship, state practice and *opinio juris*, it can be concluded that cyber operations capable of constituting resort to armed force, which ultimately corresponds to the concept of 'attack' in the law of armed conflict, would be suitable for triggering an armed conflict.[130]

[129] Pomson, O., op. cit. (ref. 81), pp. 1024-1025.

[130] It should be noted, however, that certain states associate the concept of 'hostilities', not attacks, with the existence of armed conflict. See Droit International Appliqué aux Opérations dans le Cyberspace, op. cit. (ref. 87), p. 12; On the Application of International Law in Cyberspace. Position Paper, op. cit. (ref. 88,) p. 7. According to Nils Melzer, hostilities are the collective resort to means and methods of injuring the enemy by the parties involved in the conflict. See Melzer, N.: *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva: International Committee of the Red Cross, 2009, p. 43. This concept is broader than an attack and includes unarmed information-gathering operations and pre-attack operations, thus aligning, in a broader sense, with the concept of military operations. See Melzer, N.: *Targeted Killing in International Law*, Oxford: Oxford University Press, 2008, pp. 270-272. However, this standpoint does not seem sustainable, as it would imply that any espionage activity or preparation for military operations could potentially trigger an armed conflict. It can also be argued that the two mentioned states did not necessarily base their arguments on Melzer's definition of hostilities. For example, Germany emphasizes that gaining unauthorized access to a foreign network and extracting data from it does not qualify as an attack, although it would be considered part of Melzer's definition of hostilities. Although not explicit, I doubt that Germany would characterize behaviour that does not qualify as an attack as an armed conflict. Similarly, France argues with a similar logic that various intelligence operations or operations that disrupt the enemy's ability to influence do not constitute an attack, but they are subject to the law of armed conflict. See On the Application of International Law in Cyberspace. Position Paper, op. cit. (ref. 88), p. 8. See Droit International Appliqué aux Opérations dans le Cyberspace, op. cit. (ref. 87), p. 13. Similarly, the author doubts that France would consider a cyber operation that falls below the threshold of an attack as a triggering factor for an armed conflict. The French and German positions may have drawn inspiration from the language used in the Tallinn Manual, as the international experts also associated hostilities with the existence of IACs. However, it is also revealing that

However, there is no consensus in the literature or state practice on what precisely constitutes an attack, and which cyber operations can produce the aforementioned effects. Essentially, two major viewpoints can be distinguished both in scholarship and state practice: one viewpoint argues that physical damage is necessary for an attack, which may also entail functionality loss. In such cases, repairing or replacing a physical component is necessary to restore normal functioning. The other viewpoint holds that functionality loss results in an attack even if the error can be remedied solely by reconstructing data, such as reinstalling software. However, it is worth considering to what extent physical damage and/or functionality loss corresponds to contemporary attacks in cyberspace.

For example, in 2022, two ransomware attacks hit Costa Rica, which affected the state's Virtual Tax Administration, Customs Information System, and other government websites and systems. The attacks were allegedly committed by Russia based organizations, the Conti Group and the Hive Group. The operations were aimed at disabling and shutting down systems, defacing websites, and stealing information. As typical of ransomeware attacks, the organizations demanded ruffly $25 millions (US) combined. Costa Rica refused to pay the ransom, and the attacks ultimately caused $125 million (US) in damage within the first 48 hours of the operations. Besides financial losses, health officials were unable to access medical records, or track the spread of COVID-19. These attacks, despite their serious consequences would certainly not qualify as attacks according to physical damage as a requirement viewpoint, and a significant portion of them is also not covered by the functionality loss approach – this largely depends on the technical method through which the affected systems were restored. Nevertheless, the extent of the damage caused, the state of emergency declared, and the 'state of war' communicated by the government raise concerns and prompt consideration as to whether it would be worthwhile to thoroughly reconsider the evaluation of attacks in cyberspace under IHL.[131]

At present, neither scholarship nor state practice provide definitive answers to these questions. Therefore, the future state practice (accepted as law) must guide us in interpreting (treaty law) and identifying (customary international law) these crucial rules of IHL. Without such guidance, the factual uncertainties in cyberspace may be complemented by legal uncertainties as well. In the

the participating experts could not agree on the assessment of the Stuxnet incident mentioned earlier. This indicates that it is more appropriate to seek the applicability of IHL in the context of attacks rather than hostilities. See Schmitt, M. N., op. cit. (ref. 8), pp. 383-384.

[131] <https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)>. <https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083>.

absence of a more conclusive and unified position from states to the contrary, the article argues that traditional interpretation of IHL (*i.e.* attack requires some form of physical damage) is still authoritative for states. It is also worth noting, that this conclusion stems from the well-established principles of international law, that binding norms for states are generally created through the limitation of their sovereignity, whether it is participation in a treaty, or not becoming persistent objectors regarding a particular custom. Changing such norms is a long, delicate procedure that can only happen through the cooperation of states and at the very least, with a common understanding of key international legal concepts such as attacks. Unique national state positions in and of themselves are not capable of reaching this goal.

If the application and interpretation of IHL in cyberspace remains as it is, it opens up the possibility of states conducting harmful cyber operations against each other, that can have equivalent or even more serious consquences than a "simple" kinetic operation. The problem does not lie in the possibility of launching such attacks, on the contrary, IHL would not necessarily prohibit such conduct, however, in the absence of IHL, states would not have to respect fundamental principles of hostilities, such as distinction or proportionality. The way forward, in the author's opinion, is without doubt cooperation of the members of the international community that can provide much needed common ground to apply and integrate IHL in cyberspace.

Finally, the author thinks that it would be more appropriate to use the term 'attack in cyberspace' instead of 'cyber attack' to describe the concept of 'attack' in the law of armed conflicts taking place in the cyber domain. This is because we often encounter the use of the term 'cyber attack' to describe other, fundamentally different phenomena as well.

LITERATURE

1. <https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)>, last accessed on 10/11/2024.
2. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf>, last accessed on 10/11/2024.
3. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf>, last accessed on 10/11/2024.
4. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Documento_de_posici%C3%B3n_

de_Cuba._Aplicaci%C3%B3n_del_Derecho_Internacional_a_las_TIC_en_el_ciberespacio..pdf>, last accesesed on 10/11/2024.

5. <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf>, last accessed on 10/11/2024.
6. <https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html>, last accessed on 10/11/2024.
7. <https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>, last accessed on 10/11/2024.
8. <https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf>, last accessed on 10/11/2024.
9. <https://nakeecurity.sophos.com/2011/04/26/memories-of-the-chernobyl-virus>, last accessed on 10/11/2024.
10. <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>, last accessed on 10/11/2024.
11. <https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y>, last accessed on 10/11/2024.
12. <https://rusi.org/explore-our-research/publications/commentary/all-quiet-cyber-front-explaining-russias-limited-cyber-effects>, last accessed on 10/11/2024.
13. <https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf> last accessed on 17/04/2025.
14. <https://twitter.com/ITArmyUKR>, last accessed on 10/11/2024.
15. <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbb-de-623b-9f86-b254-07d5af3c6d85?t=1603097522727>, last accessed on 10/11/2024.
16. <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb-17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>, last accessed on 10/11/2024.
17. <https://www.bbc.com/news/technology-65250356>, last accessed on 10/11/2024.
18. <https://www.bbc.com/news/uk-wales-62442127>, last accessed on 10/11/2024.
19. <https://www.cfr.org/cyber-operations/ukrainian-it-army>, last accessed on 10/11/2024.
20. <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>, last accessed on 10/11/2024.

21. <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>, last accessed on 10/11/2024.

22. <https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf>, last accessed on 10/11/2024.

23. <https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf>, last accessed on 10/11/2024.

24. <https://www.easytechjunkie.com/what-is-the-chernobyl-virus.htm>, last accessed on 10/11/2024.

25. <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf>, last accessed on 10/11/2024.

26. <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>, last accessed on 10/11/2024.

27. <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>, last accessed on 10/11/2024.

28. <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, last accessed on 10/11/2024.

29. <https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf>, last accessed on 10/11/2024.

30. <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a14>, last accessed on 10/11/2024.

31. <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>, last accessed on 10/11/2024.

32. <https://www.mofa.go.jp/files/100200935.pdf>, last accessed on 10/11/2024.

33. <https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083> last accessed on 17/04/2025

34. <https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>, last accessed on 10/11/2024.

35. <https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state>, last accessed on 10/11/2024.

36. 31st International Conference of Red Cross and Red Crescent, 2011, 31IC/11/5.1.2.

37. Akende, D., Coco, C., de Souza Dias, T.: Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies, *International Law Studies*, 99(1) 2022.

38. Arimatsu, L.: Classifying cyber warfare, in: Tsagourias, N., Buchan R. (eds.): *Research Handbook on International Law and Cyberspace* (pp. 406-426), Northampton: Edward Elgar Publishing Inc., 2021.
    - DOI: https://doi.org/10.4337/9781789904253.00031

39. Biggio, G.: The Legal Status and Targetability of Hacker Groups in the Russia-Ukraine Cyber Conflict, *Journal of International Humanitarian Legal Studies*, 15(1) 2024, pp. 142-182.
    - DOI: https://doi.org/10.1163/18781527-bja10078

40. Blank, L. R.: Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace, in: Ohlin, JD., Govern, K., Finkelstein, C. (eds.): *Cyberwar. Law and Ethics for Virtual Conflicts*, Oxford: Oxford Academic, 2015.
    - DOI: https://doi.org/10.1093/acprof:oso/9780198717492.003.0006

41. Case IT-94-1 Prosecutor v. Dusko Tadić, (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Appeals Chamber, 2 October 1995.

42. Casey-Maslen, S.: *Jus ad Bellum – The Law on Inter-State Use of Force*, Oxford: Hart Publishing, 2020.
    - DOI: https://doi.org/10.5040/9781509930722

43. Charter of the United Nations.

44. Dinstein Y.: *The Conduct of Hositilities under the Law of International Armed Conflict,* 3rd edn, Cambridge: Cambridge University Press, 2016.
    - DOI: https://doi.org/10.1017/CBO9781316389591

45. Dinstein, Y., Dahl, A. W.: O*slo Manual on Select Topics of the Law of Armed Conflict. Rules and Commentary*, Cham: Springer, 2020.
    - DOI: https://doi.org/10.1007/978-3-030-39169-0

46. Dinstein, Y.: *War, Agression and Self-Defence*, 5th edition, Cambridge: Cambridge University Press, 2011.
    - DOI: https://doi.org/10.1017/CBO9780511920622

47. Droege, C.: Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians, *International Review of the Red Cross*, 94(886) 2012, pp. 533-578.
    - DOI: https://doi.org/10.1017/S1816383113000246

48. Egloff, F. J., Shires, J.: Offensive Cyber Capacities and State Violence: Three Logics of Integration, *Journal of Global Security Studies*, 7(1) 2021.
    - DOI: https://doi.org/10.1093/jogss/ogab028

49. Eilstrup-Sangiovanni, M.: Why the World Needs an International Cyberwar Convention, *Philosophy & Technology*, 31(3) 2018, pp. 379-407.
- DOI: https://doi.org/10.1007/s13347-017-0271-5

50. Engdahl, O., Sweden's Position Paper on the Application of International Law in Cyberspace, *Nordic Journal of International Law,* 92(3) 2023, pp. 489-497.
- DOI: https://doi.org/10.1163/15718107-20230004

51. Geneva Convention relative to the Protection of Civilian Persons in Time of War, 12 August 1949.

52. Grignon, J.: The Beginning of Application of International Humanitarian Law: A Discussion of a Few Challenges, *International Review of the Red Cross*, 96(893) 2014, pp. 139-162.
- DOI: https://doi.org/10.1017/S1816383115000326

53. Herczegh, G.: *A humanitárius nemzetközi jog fejlődése és mai problémái*, Budapest: Közgazdaság lap- és könyvkiadó, 1981.

54. Hoffmann, T.: War or peace? - International legal issues concerning the use of force in the Russia-Ukraine conflict, *Hungarian Journal of Legal Studies*, 63(3) 2022, pp. 206-235.
- DOI: https://doi.org/10.1556/2052.2022.00419

55. ICRC: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), Geneva: ICRC, 1949.

56. International Committee of the Red Cross: *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, Cambridge: Cambridge University Press, 2016.

57. International Committee of the Red Cross: 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*, 102(913) 2020, pp. 481-492.
- DOI: https://doi.org/10.1017/S1816383120000478

58. International Committee of the Red Cross: *International humanitarian law and the challenges of contemporary armed conflicts report*, Geneva: International Committee of the Red Cross, 32IC/15/11, October 2015.

59. International Committee of the Red Cross: *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 8 June 1977*, Geneva: International Committee of the Red cross, May 2010.

60. International Committee of the Red Cross: *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, 27.12.2022.

61. International Court of Justice: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, *ICJ Reports*, 1996.

62. International Court of Justice: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986.

63. International Court of Justice: *North Sea Continental Shelf, Judgment*, ICJ Reports 1969.

64. International Court of Justice: Statute of the International Court of Justice, <https://www.icj-cij.org/statute>, last accessed on 10/11/2024.

65. Kajtár, G.: *Betudás a nemzetközi jogban. A másodlagos normák szerepe a beruházásvédelemtől a humanitárius jogig*, Budapest: ORAC, 2022.

66. Kis Kelemen, B.: *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására*, Pécs: Publikon Kiado, 2023.
    - DOI: https://doi.org/10.51783/ajt.2023.3.06

67. Kis Kelemen, B.: Nemzetközi fegyveres konfliktusok a kibertérben, *Közjogi Szemle*, (3) 2023, pp. 39-47.

68. Kis Kelemen, B.: Protection of (Personal) Data in Armed Conflicts, *Baltic Journal of Law & Politics*, 17(1) 2024, pp. 1- 20.
    - DOI: https://doi.org/10.2478/bjlp-2024-0001

69. Kittichaisaree, K.: *Public International Law of Cyberspace*, Cham: Springer, 2017.
    - DOI: https://doi.org/10.1007/978-3-319-54657-5

70. Kjelgaard, J. M., Melgaard, U.: Denmark's Position Paper on the Application of International Law in Cyberspace, *Nordic Journal of International Law*, 92(3) 2023, pp. 446-455.
    - DOI: https://doi.org/10.1163/15718107-20230001

71. Koh, H. H.: International Law in Cyberspace. Remarks Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD. Sept. 18, 2012, *Harvard International Law Journal,* 54(1) 2012.

72. Korzak, E., Gow, J.: Computer network attacks under the jus ad bellum and the jus in bello. 'Armed' – effects and consequences', in: Gow, J., Dijxhoorn, E., Kerr, R., Verdirame, G. (eds.): *Routledge Handbook of War, Law and Technology*, New York: Routledge, 2021.

73. Letho, M.: Finland's views on International Law and Cyberspace, *Nordic Journal of International Law,* 92(3) 2023, pp. 456-469.
    - DOI: https://doi.org/10.1163/15718107-20230002

74. Mačák, K.: 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.

75. Manual of the Law of Armed Conflict, Norway, 2013.

76. McReynolds, P.: How to Think About Cyber Conflicts Involving Non-state actors, *Philosophy & Technology,* 28(3) 2015, pp. 427-448.
    - DOI: https://doi.org/10.1007/s13347-015-0187-x

77. Melzer, N.: *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva: International Committee of the Red Cross, 2009.

78. Melzer, N.: *Targeted Killing in International Law*, Oxford: Oxford University Press, 2008.
    - DOI: https://doi.org/10.1093/acprof:oso/9780199533169.001.0001

79. Musæus, V.: Norway's Position Paper on International Law and Cyberspace, *Nordic Journal of International Law*, 92(3) 2023, pp. 470-488.
    - DOI: https://doi.org/10.1163/15718107-20230003

80. Oppenheim, L.: *International Law a Treatise*, 2nd edition, London: Longmas Green, 1926.

81. Pictet, J.: *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field,* Geneva: ICRC, 1952.

82. Pomson, O., Methodology of identifying customary international law to cyber activities, *Leiden Journal of International Law*, 36(4) 2023, pp. 1023-1047.
    - DOI: https://doi.org/10.1017/S0922156523000390

83. Pomson, O.: 'Objects'? The Legal Status of Computer Data under International Humanitarian Law, *Journal of Conflict & Security Law*, 28(2) 2023, pp. 349-387.
    - DOI: https://doi.org/10.1093/jcsl/krad002

84. Quintin, A.: Attacks, in: Djukić, D., Pons N. (eds.): *The Companion to International Humanitarian Law*, Leiden: BRILL, 2018.

85. Roscini, M.: *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014.
    - DOI: https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

86. Sandoz, Y., Swinarski, C., Zimmermann, B. (eds.): *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva: Oxford University Press, 1987.

87. Schack, M., Lund-Hansen, K., Attacking Data: Moving beyond the Interpretative Quagmire of the 'Data as an object', *Nordic Journal of International Law*, 92(3) 2023, pp. 349-370.
    - DOI: https://doi.org/10.1163/15718107-92030004

88. Schmitt, M. N. (ed.): *Tallin Manual 2.0 On the International Law Applicable to Cyber Operations*, New York: Cambridge University Press, 2017.
- DOI: https://doi.org/10.1017/9781316822524

89. Schöndorf, R.: Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, *International Law Studies*, 97(1) 2021.

90. Stahn, C.: 'Jus ad bellum', 'jus in bello' ... 'jus post bellum'? – Rethinking the Conception of the Law of Armed Force, *European Journal of International Law*, 17(5) 2006, pp. 921-943.
- DOI: https://doi.org/10.1093/ejil/chl037

91. United Nations General Assembly: *Official compendium of voluntary national contributions on the subject of how international law applies 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 resolution 73/266*, United Nations General Assembly, 13.07.2021.

92. United Nations Security Council: *Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*, New York: United Nations, 24 February 2022.

93. Weizmann, N.: Armed Drones and the Law of Armed Conflict, in: Casey-Maslen, S., Homayounnejad, M., Stauffer, H., Weizmann, N. (eds.): *Drones and Other Unmanned Weapons Systems under International Law* (pp. 89-122), Leiden: KONINKLIJKE BRILL NV, 2018.
- DOI: https://doi.org/10.1163/9789004363267_006

94. Yoo, C. S.: Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures, in: Ohlin, JD., Govern, K., Finkelstein, C. (eds.): *Cyberwar. Law and Ethics for Virtual Conflicts* (pp. 175-194), Oxford: Oxford Academic, 2015.
- DOI: https://doi.org/10.1093/acprof:oso/9780198717492.003.0009