„Krytyka Prawa", tom 18, nr 2/2026, s. 236–259, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Author.

BENCE KIS KELEMEN[1]

Civilian Participation in Cyber Conflicts with a Particular Focus on Hacking[2]

Submitted: 08.01.2025. Accepted: 20.04.2026

Abstract

Civilian involvement in armed conflicts has become easier because of new technologies, as anyone with a smartphone can share critical military information, engage in hacking, and other cyber operations. This raises concerns, especially if individuals are unaware that their actions may have serious consequences. International humanitarian law protects civilians from attacks unless, and for such time as, they take a direct part in hostilities. Clear rules are essential, particularly for cyber operations. This article explores civilian participation in cyber conflicts, with hacking as a key example, highlighting issues in the interpretation of applicable law and comparing the relevant legal approaches with state practices. It concludes that states should develop clearer guidelines to address civilian roles in cyber conflicts effectively.

Keywords: direct participation in hostilities (DPH), cyber conflict, hacking, Tallinn Manual, national positions.

[1] Bence Kis Kelemen – University of Pécs, Faculty of Law, Department of International and European Law (Hungary); e-mail: kis.kelemen.bence@ajk.pte.hu; ORCID: 0000-0001-9641-1557.

[2] The research in this article has not been supported financially by any institution.

„Krytyka Prawa", tom 18, nr 2/2026, s. 236–259, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Author.

BENCE KIS KELEMEN

Udział ludności cywilnej w konfliktach cybernetycznych ze szczególnym uwzględnieniem hakowania[3]

Streszczenie

Udział cywilów w konfliktach zbrojnych stał się łatwiejszy za sprawą nowych technologii, ponieważ niemal każda osoba mająca smartfon może przekazywać istotne informacje o znaczeniu wojskowym. Rodzi to poważne obawy, zwłaszcza w sytuacjach, gdy osoby te nie zdają sobie sprawy, że ich działania mogą mieć daleko idące konsekwencje. Międzynarodowe prawo humanitarne chroni cywilów przed atakiem, chyba że – i przez taki czas, w jakim – biorą oni bezpośredni udział w działaniach zbrojnych. Jasne zasady są szczególnie istotne w odniesieniu do operacji cybernetycznych. W niniejszym artykule autor analizuje udział cywilów w konfliktach cybernetycznych, ze szczególnym uwzględnieniem działań hakerskich, wskazując na problemy związane z interpretacją właściwych norm prawnych oraz zestawiając je z praktyką państw. W konkluzji podkreślono, że państwa powinny wypracować bardziej klarowne wytyczne dotyczące roli cywilów w konfliktach cybernetycznych.

Słowa kluczowe: bezpośredni udział w działaniach zbrojnych (DPH), konflikt cybernetyczny, działania hakerskie, Podręcznik talliński, stanowiska państw.

[3] Badania opisane w tym artykule nie zostały sfinansowane przez żadną instytucję.

 DOI: 10.7206/kp.2080-1084.860

Introduction

In contemporary armed conflicts, new technologies are used with increasing intensity both by the parties to those conflicts and by individuals and entities supporting these organisations. To mention only two such examples, reference can be made to the targeted killing policies and practices of many states, in which unmanned aerial vehicles – more commonly known as drones – are used,[4] there is also a growing concern about the use of fully autonomous weapons systems in armed conflicts, which are no longer the realm of science fiction.[5] The scope of this article, however, is different, as it focuses on a third category of new technologies employed in armed conflicts, namely cyber operations.

State-sponsored cyber operations have been on the rise for many years now[6]. Once again, two examples may be drawn from the broader category of hostile operations, even if they are not necessarily state-sponsored. One of the best-known hostile cyber operations took place in Iran, allegedly as a result of cooperation between the United States of America and Israel. The operation employed malware known as "Stuxnet," which subsequently caused physical damage to Iranian uranium enrichment facilities in 2010.[7] A lesser-known example is connected to the Russo-Ukrainian armed conflict, in which an organisation called the "Cyber Partisans of Belarus" claimed responsibility for launching a ransomware attack against the Belarusian railway system in 2022, which was used by Russian troops[8] to support their "special military operation," – or, more accurately, Russia's aggression

4 B. Kis Kelemen, *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására,* Pécs 2023; N. Melzer, *Targeted Killing in International Law*, Oxford 2008.

5 J. Saballa, *Anduril Introduces Bolt-M Autonomous Attack Drone*, "The Defense Post", 11 October 2024. Available from: https://thedefensepost.com/2024/10/11/anduril-bolt-attack-drone/ (accessed: 15.10.2024); B. Schubert, *Az fegyverrendszerekkel szemben támasztott követelmények a humanitárius nemzetközi jog tükrében*, "Honvédségi Szemle" 2022, 3, pp. 20–30; E.H. Ma, *Autonomous Weapons Systems under International Law*, "New York University Law Review" 2020, 5, pp. 1435–1474.

6 *Cyber Operations Tracker*, Council on Foreign Relations. Available from: https://www.cfr.org/cyber-operations/ (accessed: 15.10.2024).

7 *Stuxnet*, "Britannica". Available from: https://www.britannica.com/technology/Stuxnet (accessed: 15.10.2024).

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

against Ukraine[9] – on the northern front. Hence, it can be argued that hackers provide states with a low-cost opportunity to project their power in cyberspace.[10]

This latter example brings the discussion to the scope of this article, namely hacking as direct participation in hostilities (DPH) in contemporary armed conflicts. DPH is a core concept of international humanitarian law (IHL). It is well established that civilians enjoy general protection from the harmful effects of armed conflicts. This translates, among other things, into a prohibition on direct attacks against civilians.[11] There are, however, situations in which such protection cannot logically be maintained, for instance, when a civilian takes up arms against the adversary and participates in the conflict. DPH therefore entails the suspension of the protection mentioned above for the duration of direct participation in the hostilities.[12] Examples of direct participation include killing and wounding military personnel and disrupting deployment, logistics, and communications.[13] The Russo-Ukrainian armed conflict has shown that civilians are increasingly interested in participating in ongoing conflicts in any way they can. The Cyber Partisans of Belarus are just one example illustrating this point. The organisation can be considered a collective of hacktivists primarily opposed to the current government of Belarus, while also supporting Ukraine in its war effort[14] against the Russian Federation.[15] Ukraine also called upon its own "cyber army", which developed into the so-called "IT Army of Ukraine", whose members are not necessarily only Ukrainian nationals and whose goal is to conduct cyber operations against Russian targets.[16] Individual civilians can also participate in the war effort simply by downloading certain applications, such as "eVorog" or "ePPO", which serve as tools for transmitting information. They can report Russian troop locations and movements, or even missiles and kamikaze drones for subsequent targeting by the

9 T. Hoffmann, *War or peace? – International legal issues concerning the use of force in the Russia–Ukraine conflict*, "Hungarian Journal of Legal Studies" 2022, 3, pp. 206–235.

10 J. Vastoupal, K. Uhlířová, *Of Hackers and Privateers: The Possible Evolution of Cyber Attribution*, „Masaryk University Journal of Law and Technology" 2024, 2, p. 192.

11 Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) UNTS: 17512 (AP I) Article 51(1)-(2).

12 AP I Article 51(3)

13 N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* Geneva 2009, p. 48.

14 Please note, that the language „war effort" in Section I is used in a purely grammatical context, without any legal significance, as the difference between participating in a war effort and direct participation in hostilities will be shown in Section II.

15 G. Biggio, *op. cit.*, pp. 146–147.

16 R. Buchan, N. Tsagourias, Ukranian *'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?*, "EJIL:Talk!" 9 March 2022. Available from: https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ (accessed: 15.10.2024).

 DOI: 10.7206/kp.2080-1084.860

Ukrainian armed forces.[17] This phenomenon has recently been described in the literature as "Crowdsourced War", a term that also covers social media recruiting, crowdfunding, open-source intelligence gathering, and the use of the Starlink system.[18] Direct participation and Crowdsourced War are connected because civilians who participate in a crowdsourced war might qualify as direct participants, and consequently, might lose the protection afforded to them by international law. To illustrate the potentially deadly consequences of linking the two phenomena, one can recall the case of Hennadiy Merchynskyi, who was executed by Russian troops in the Ukrainian village of Motyzhyn because pictures of Russian tanks were found on his phone[19].

Against this background, it is not surprising, that the International Committee of the Red Cross (ICRC) has published 8 rules for civilian hackers and 4 obligations for states to restrain them in 2023.[20] The importance of these rules can be illustrated by the fact, that the IT Army of Ukraine has already endorsed them, whereas the Russian hacker group "Killnet" has outright rejected the applicability of these principles.[21]

A common feature of all organisations mentioned so far is that they have no official state affiliation, meaning that they have not been incorporated into the armed forces of any state. This means that their members do not necessarily have traditional combatant status, which in turn leaves them as civilians in the context of an armed confrontation. According to the traditional understanding of the definition, a civilian is someone who is not a member of the armed forces of a party to the conflict or a participant in a levée en masse.[22] These three categories are mutually exclusive, meaning that a person affected by the conflict must fall into one of these groups.[23] As was illustrated above, it is well established among military professionals and international lawyers, that civilians who directly participate in hostilities lose their protection against being targeted in an armed conflict;[24] however, the precise scope of such participation and its consequences remains

17 G. Biggio, *op. cit.*, p. 148.

18 O.A. Hathaway, I. Pe'er, C. Vera, *Crowdsourced war,* „New York University Law Review" 2025, 100.

19 *Ibidem,* p. 1565.

20 T. Rodenhäuser, M. Vignati, *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them*, "Humanitarian Law & Policy" 4 October 2023. Available from: https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ (accessed: 15.10.2024).

21 C. Jones, *Red Cross lays down hacktivism law as Ukraine war rages on*, "The Register" 4 October 2023, https://www.theregister.com/2023/10/04/red_cross_hacktivist_rules/ (accessed: 15.10.2024).

22 AP I I Article 50.

23 N. Melzer, *Interpretive Guidance…*, pp. 20–21.

24 AP I Article 51(3).

controversial. Many scholars identify grey areas in which the line between a civilian and a direct participant in hostilities seems to blur. Examples include a person posting notice of a vulnerability in an open-source computer operating system that can later be exploited in an attack, a civilian contractor identifying such a vulnerability, or a third person introducing malware that utilizes the identified vulnerability for future use.[25]

Based on this, several legal questions can be posed: (i) what acts constitute direct participation in hostilities in the cyber context, (ii) what is the temporal scope of such participation, and (iii) does the organisation within whose framework this happens matter in international armed conflicts?

This article has a limited scope. It seeks to explore the above legal questions in more detail and briefly highlight the differences and their consequences in the literature and practice (Section II). It then examines state practice accepted as law in the form of national positions published by states on the applicability of international law to cyber operations (Section III). Finally, the paper offers some concluding remarks regarding the applicability of IHL to the issue of direct participation in hacking-type cyber operations (Section IV). The article therefore does not investigate how the conduct of civilian hackers interacts with other branches of international law, such as the law governing the use of force as regulated by the United Nations Charter and general international law, nor does it reflect on human rights obligations in light of civilian participation in cyber-related armed conflicts.

The Applicable Law on Hacking as Direct Participation and Its Contentious Issues

The modern international treaties applicable to armed conflicts are the four 1949 Geneva Conventions, which have been virtually universally ratified, and their 1977 Additional Protocols, which are less widely accepted.[26] The first 1977 Additional Protocol (AP I), which regulates international armed conflicts, in Article 51(3) states that:

---

25 K. Kittichaisaree, *Public International Law of Cyberspace,* Cham 2017, p. 219.

26 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, UNTS: 970; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, UNTS: 971; Geneva Convention Relative to the Treatment of Prisoners of War, UNTS: 972; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, UNTS: 973. AP I; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of non-international armed conflicts (Protocol II) UNTS: 17513.

 DOI: 10.7206/kp.2080-1084.860

> "Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities."[27]

The same rule can be inferred from Common Article 3(1) of the 1949 Geneva Conventions, which refers to persons who take no active part in hostilities.[28] This rule of IHL means that although civilians generally enjoy protection from the dangers arising from the military operations,[29] and the civilian population – like individual civilians – may not be the direct target of an attack,[30] this protection is lost if a civilian takes a direct part in hostilities, for the duration of such direct participation. The same rule seems to be reflected in customary international law as well.[31]

The 1987 Commentary on AP I makes several observations regarding direct participation. First, hostile acts are those which, by their nature and purpose, are designed to cause actual harm to the adversary.[32] This includes preparatory and concluding acts as well,[33] and it should be more than merely participating in the war effort of a party to the conflict.[34] Naturally, the clarification provided in the original commentary seems inadequate for such an important rule of IHL in complex battlespaces like the cyber realm.

To address this problem in part, the ICRC, in cooperation with the T.M.C. Asser Institute, attempted to develop a common position on the notion of DPH. The work began in 2003, but a significant number of experts later withdrew from the initiative.[35] At the end of the process, the ICRC published its Interpretive Guidance (IG) on the issue, authored by Nils Melzer.[36] As noted, the IG attracted significant criticism. One of the arguments raised by a significant number of experts was that, according to the IG's recommendation, force should be used, even against combatants,

---

27 AP I, Article 51(3).

28 Common Article 3(1) of the Geneva Conventions referred to in footnote n. 26.

29 AP I, Article 51(1).

30 AP I, Article 51(2). indirect civilian casualties are still possible AP I, Article 51(5)(b).

31 J. M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law. Volume I. Rules*, Cambridge 2009, pp. 19–24, Rule 6.

32 *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ed. Yves Sandoz et al, Geneva 1987, para. 1942.

33 *Ibidem*, para. 1943.

34 *Ibidem*, para. 1945.

35 K. Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance,* "New York University Journal of International Law and Politics" 2010, 1, pp. 641–695; W. Boothby, *And for Such Time as: The Time Dimension to Direct Participation in Hostilities*, "New York University Journal of International Law and Politics" 2010, 1, pp. 741–768; W. H. Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, "New York University Journal of International Law and Politics" 2010, 1, pp. 769–830.

36 N. Melzer, *Interpretive Guidance…*

only to the extent that is actually necessary to accomplish a legitimate military purpose in the circumstances.[37] For example, according to W. Hays Parks – a view shared by at least 15 experts – no such obligation can be identified in international humanitarian law; such an obligation is unworkable and contrary to state practice.[38] The ICRC also offered its explanation for the inclusion of this recommendation. According to that explanation, this rule would serve as a counterbalance to the notion of continuous combat function and was not meant to be used in large-scale confrontations, but rather in relation to individuals under the territorial control of the state who could be apprehended.[39] Another strand of criticism came from William Boothby, who argued that the temporal scope of DPH was misconstrued, creating too narrow a window of targetability;[40] furthermore, non-members of armed groups who regularly participate in the conflict could still "escape through the revolving-door".[41] Some were critical of the formulation of the membership criteria, while others opposed the way in which the IG addressed the issue of voluntary human shields and hostage-taking.[42] It needs to be noted that, while there is significant opposition to the content of the IG's position, as will be seen below, states have – at least to some extent – internalised the ICRC's concepts. Hence, in my opinion, the Interpretive Guidance can be accepted as a reasonably accurate account of the law, given its recognition in scholarship and state practice, at least with respect to the basic principles of DPH. It is always possible to analyse the notion of DPH further, but the aim of this article is not to resolve the decades--old controversies regarding the concept, but rather to introduce this notion in the context of cyber operations and offer a detailed analysis of how states engage with the topic in the cyber domain. Therefore, the IG will be used to illustrate the notion of direct participation in hostilities.

The IG uses three cumulative criteria for determining who is to be considered a direct participant in hostilities. The first criterion is the "threshold of harm", according to which "the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack[43]." The

37 N. Melzer, *Interpretive Guidance…*, Recommendation IX.

38 W.H. Parks, *op. cit*., p. 785; E. Crawford, *Identifiying the Enemy. Civilian Participation in Armed Conflict*, Oxford 2015, p. 83.

39 E. Crawford, *op. cit*., pp. 83–84.

40 According to Boothby, preparatory actions with the aim of estabishing a general capacity to carry out hostile acts is DPH contrary to the IG's position. For instance, hiding a weapon with a view to further hostilities is still direct participation. W. Boothby, *op. cit.,* pp. 746–750.

41 W. Boothby, *op. cit.,* p. 743.

42 K. Watkin*, op. cit*.; E. Crawford, *op. cit.,* pp. 84–85.

43 *Ibidem*, p. 46.

 DOI: 10.7206/kp.2080-1084.860

IG also illustrates this with several examples: sabotage, the restriction or disruption of deployment, or the denial of military use of certain objects, equipment, and territory.[44] It seems that the cyber operation against the Belarusian railway system, which hindered the movement of Russian troops, meets the threshold of harm criterion. The same might arguably be true for a denial-of-service (DoS) attack that would block the military use of a given satellite or a military network. Although the IG does not use the term "cyber operation," it specifically states, that "[e]lectronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack. "[45] However, mere manipulation of computer networks, without adverse military effects, will not amount to direct participation.[46]

The second criterion that must be fulfilled is "direct causation", which means that the action and the result should not be further apart than one causal step. Meaning, capacity-building or causing harm indirectly will fall outside the scope of DPH.[47] According to some international law scholars, the direct causation is still present if the acts form an integrated chain of events, and the result – that is, the harm – would not have occurred but for the cyber operation itself.[48] In my view, this does not necessarily create a causality problem for cyberattacks. Naturally, no state would question that if a cyber operation were to shut down a hospital, and as an indirect result, patients died due to inadequate care, it would almost certainly qualify as an attack under IHL.[49] If we allow such a broad version of causality for one kind of DPH, then why would we deny the direct participant status to a person, who denies access to a satellite system and, as an also indirect result, considerably slows military deployment, for example because some troops get lost, or the coordination requires more time? Yet, many experts seem to be sceptical about this aspect of DPH. They point out that already in 2008, during the Russo-Georgian War, Russian websites provided instructions for DDoS attacks. Similarly, a civilian who writes malware and gives it to the armed forces will most likely not to fall into the category of "direct causation," which in turn would leave such individuals outside the scope of DPH.[50]

---

44 *Ibidem*, p. 48.

45 *Ibidem*.

46 *Ibidem*, p. 50.

47 *Ibidem*, pp. 52–53.

48 G. Biggio, *op. cit.*, p. 168.

49 L. Gisel, T. Rodenhäuser, K. Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, „International Review of the Red Cross" 2020, 102, p. 313.

50 E. Crawford, *op. cit.*, pp. 147–148.

Lastly, the third criterion is belligerent nexus, which requires the act to be specifically designed to cause the harm identified above, with the purpose of supporting one party and acting to the detriment of another.[51] This refers to the objective purpose of the act, rather than the subjective intent of the individual.[52]

To revisit the critical arguments mentioned above, at least to some extent, it is useful to note, that according to the IG, "[w]here the execution of a hostile act does not require geographic displacement, as may be the case with computer network attacks […], the duration of direct participation in hostilities will be restricted to the immediate execution of the act and preparatory measures forming an integral part of that act."[53] Contrary to this view, Parks notes, that the inclusion of language such as "integral" is a misinterpretation of the law, since, in his view, all preparatory acts should be regarded as DPH.[54] Others also consider the same problem in the context of what kinds of cyber activities qualify as the conduct of hostilities. Julia Dornbusch, for example, claims that infecting civilian systems with malware can be seen as a preparatory act that is also part of the attack itself, in which context even proportionality questions can arise.[55] From a practical perspective, these debates regarding cyber operations appear somewhat artificial. When it comes to lone-wolf hackers, a state will not be in a position to recognise that a cyber operation is about to take place or to identify the person behind it. According to the European Repository of Cyber Incidents, more than 54% of all cyber operations are either not attributed to anyone or involve an unknown perpetrator.[56] Furthermore, industry and political attribution still take more than 2 months as of December 2025[57]. Given these numbers, it seems rather unrealistic to assume that the attacker can be identified in the preparatory phase. In the case of continuous combat function, this problem is once again a non-issue, since then targetability remains effective for the duration of the individual's functional membership in the organisation.[58]

Before turning to specific cyber-related international legal literature, it should be noted that there is a broad consensus in the international community as to the

---

51 N. Melzer, *Interpretive Guidance…*, p. 58.

52 B. Kis Kelemen, *Human Shielding, Subjective Intent, and Harm to the Enemy,* "Journal of Conflict & Security Law" 2020, 3, pp. 537–564.

53 N. Melzer, *Interpretive Guidance…*, p. 68.

54 W.H. Parks, *op. cit.*, p. 752.

55 J. Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg,* Köln 2018, pp. 144–145.

56 *From where to where are cyber incidents most frequently initiated and received? (Bar Chart),* "European Repository of Cyber Incidents". Available from: https://eurepoc.eu/dashboard/ (accessed:15.10.2025).

57 *How long does it take for the initiator of a cyber incident to be attributed? (Attribution speed)*, "European Repository of Cyber Incidents" https://eurepoc.eu/dashboard/ (accessed: 15.10.2025).

58 N. Melzer, *Interpretive Guidance…*, pp. 34 and 72.

 DOI: 10.7206/kp.2080-1084.860

applicability of international law in cyberspace.[59] This was reaffirmed in 2021 by the United Nations Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[60] The GGE also called for further study on how and when IHL principles apply in cyberspace.[61] The need for capacity-building in the areas of international law, national legislation, and policy was also underlined by the United Nations Open--ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[62] No such consensus can be found, however, when it comes to the applicability of IHL to cyber operations[63] or the form of that applicability.[64] Despite this, international law seems to be clear on at least the applicability issue: the International Court of Justice (ICJ) in the Nuclear Weapons advisory opinion expressly stated, that IHL would be applicable to the use of new types of weapons, such as nuclear weapons.[65] Arguably, the same should be true for cyber weapons and cyber operations more generally.

Perhaps the most important scholarly work to date on the applicability of international law in cyberspace is the Tallinn Manual 2.0 (Tallinn Manual). The book should be considered a private codification effort, meaning that it does not reflect the position of any state, but rather the views of the participating experts on applicable international law.[66]

The Tallinn Manual, in Rule 97, reiterates Article 51(3) of AP I, stating that civilians enjoy protection from attack as long as they are not directly participating

---

59 *International humanitarian law and the challenges of contemporary armed conflicts report*, International Committee of the Red Cross, October 2015., p. 39. Available from: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts (accesssed: 15.10.2024).

60 United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. A/76/135. 14 July 2021. para 69.

61 *Ibidem*, para 71. (f)

62 United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, A/AC.290/2021/CRP.2 10 March 2021. para 37.

63 K. Mačák, *This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace*, "Exeter Centre for International Law Working Paper Series" 2019, 2, p. 3.

64 See e.g. issues regarding the object status of electronic data. See B. Kis Kelemen, *Protection of (Personal) Data in Armed Conflicts*, "Baltic Journal of Law & Politics" 2024, 1, pp. 4–9. Domain specific rules might also be applicable according to some states, See D. Akande, A. Coco, T. de Souza Dias, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies*, "International Law Studies" 2022, 1, p. 8. The authors, however, do not agree with such a position. See *ibidem,* p. 12.

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

66 M. Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, "Just Security" 9 February 2017. Available from: https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ (accessed: 16.10.2024); M. Kiss, *Kibertűveletek a beavatkozás tilalma mint nemzetközi jogi alapelv tükrében*, "Állam- és Jogtudomány" 2023, 4, p. 72.

in hostilities[67]. The Tallinn Manual highlights that for direct participation to occur an act is always required, which presupposes intention, meaning that involuntary participation, for example through a botnet, will not create DPH status.[68] Most of the experts agreed with the IG, claiming that a negative effect on the adversary's military is necessary; however some experts were of the view that enhancing one's own cyber capabilities would also suffice.[69] The Tallinn Manual also offered examples of direct participation, such as cyberattacks, making attacks possible, for instance, through malware, distributed denial of service attacks, gathering information and passing it on to the state armed forces. However, the mere designing of malware and making it public, or maintaining computer equipment, will not amount to direct participation. The experts were divided on the issue of malware development in cases where the target was not known by the supplier.[70] The experts agreed that preparatory and immediately subsequent acts were part of direct participation, but the precise temporal scope of participation remained open to question.[71] It should be noted here that this is contrary to the position of the IG, which states that in the case of computer network attacks (e.g. cyber operations), DPH is restricted to the immediate act and preparatory measures forming an integral part of that specific act.[72] One issue was, in the case of delayed effects, how far an individual's DPH extends in a temporal sense. The majority argued that the temporal scope is wide enough to encompass everything from the beginning of the involvement up to the termination of the individual's active role in the operation.[73] The minority, however, understood different parts of the same operation (e.g. installing and activating malware) as separate instances of direct participations.[74] The other temporal problem concerned repeated operations. The experts were divided on this issue: while some argued that targetability applies during the intermittent periods between attacks as well, others claimed that once the active role is terminated, direct participation ends.[75] It also needs to be highlighted, that the ICRC developed its own solution to the revolving door problem, which was the continuous combat function[76]. This, however, requires a separate non-

67 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. M. Schmitt, Oxford 2017, p. 428.
68 *Ibidem*, p. 429; see the contrary view regarding involuntary human shields in B. Kis Kelemen, *Human Shielding…*, 2020.
69 M. Schmitt, *Tallinn Manual 2.0…*, p. 429.
70 *Ibidem*, p. 430.
71 M. Schmitt, *Tallinn Manual 2.0 …*, p. 431.
72 N. Melzer, *Interpretive Guidance…*, p. 68.
73 M. Schmitt, *Tallinn Manual 2.0*, p. 431.
74 *Ibidem,* pp. 431–432.
75 *Ibidem,* p. 432.
76 N. Melzer, *Interpretive Guidance…*, pp. 71–72.

 DOI: 10.7206/kp.2080-1084.860

-international armed conflict between the organisation in which the individual is assumed to have a continuous combat function, the threshold of which would be rather high.[77] The experts were also divided on the issue of a presumption against direct participant status. Some argued that there is a presumption against DPH, others claimed that it only applies to civilian status, i.e. in cases of doubt, individuals should be treated as civilians.[78]

At this point, it seems useful to examine some of the problems posed by DPH through an illustrative example. As it has been mentioned above, the IT Army of Ukraine makes it possible for civilians to participate in the Russo-Ukrainian armed conflict, including individuals potentially located on the other side of the globe. The IT Army of Ukraine coordinates its hostile operations through cloud services and tools hosted on platforms such as GitHub. Its operations largely include DDoS attacks on government and banking websites, but it has also managed to shut down the computer system of Loesk, an electrical utility, which resulted in a power outage in the Leningrad region of Russia.[79] Participating in some of these operations would undoubtedly constitute DPH, resulting in the loss of protection for individuals and potential criminal liability upon capture, while others, such as a simple DDoS operation, would likely fall outside the scope of DPH. Ukraine sought to solve the problem caused by Crowdsourced War unilaterally by creating national legislation that would incorporate the IT Army of Ukraine into the state's reserve forces, thereby making its members combatants; however, the initiative has still not borne fruit.[80] In light of the above, many questions still remain; for example, would developing malware to be used later by someone else be considered direct participation? Could maintaining cyber infrastructure for defence purposes or sharing intelligence on potential targets or their vulnerabilities have the same result? A word of caution is once again in order before the issue is overstated. Although, technically, any individual who qualifies as a direct participant in hostilities might be targetable, even if located in a neutral state, the use of interstate force would still be constrained by Article 2(4) of the United Nations Charter – in other words, the prohibition on the use of force. It seems rather unrealistic that a state could claim lawful self-defence against a lone-wolf hacker, given the very high threshold of an armed attack required by international law, except perhaps in relation to the cyber operation against Loesk;[81] moreover, and no territorial

77 G. Biggio, *op. cit.*, pp. 164–165.
78 M. Schmitt, *Tallinn Manual 2.0…*, p. 432.
79 O.A. Hathaway, I. Pe'er, C. Vera, *op. cit.,* pp. 1573–1574, and p. 1611.
80 *Ibidem,* p. 1613.
81 M. Kiss, *A kiberműveletek és a jus ad bellum kapcsolata*, "Jura" 2022, 3, pp. 50–51.

state would realistically consent to the use of force on its territory, potentially against its own citizens, in this context.

At this point, the only conclusion that can be drawn with confidence is that a significant part of the literature would exclude these examples from DPH based, among other things, on the IG's assessment, while another group strongly opposes an overly narrow characterisation of the concept.[82] Based on the above, a number of contentious issues can be identified: (i) it is unclear what kind of operations will be considered harmful to the enemy, meaning that they reach the required threshold of harm; (ii) the temporal scope of the participation is also ambiguous, specifically in relation to the revolving door problem and the beginning and end of actual DPH; and (iii) the existence of a presumption against direct participation status is also uncertain. The following section, therefore, examines states' answers to these questions.

National Positions

A legal analysis in international law cannot be considered complete without an examination of state practice and corresponding opinio juris. On the one hand, the ICJ held in the North Sea Continental Shelf case that customary international law has two constitutive elements: settled state practice and the belief that such practice is followed out of a sense of legal obligation (opinio juris).[83] On the other hand, when it comes to treaty law, the general rule of interpretation in the 1969 Vienna Convention on the Law of Treaties should be complemented by "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation."[84] It is therefore of paramount importance to investigate state practice accepted as law as an interpretative tool for treaty obligations, as well as for the identification of customary international law. It should be highlighted that this article adopts Ori Pomson's view that customary international law should not be subject to interpretation, but only to identification or determination.[85]

82 O.A. Hathaway, I. Pe'er, C. Vera, *op. cit*., pp. 1611–1613.

83 See North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3, para. 77.

84 1969 Vienna Convention on the Law of Treaties, UNTS: 1155, Article 31(3)(b).

85 O. Pomson, *Methodology of identifying customary international law applicable to cyber activities*, "Leiden Journal of International Law" 2023, 4, p. 1031.

 DOI: 10.7206/kp.2080-1084.860

The scope of the research covers 36 national positions,[86] which includes not only state positions, but also the views of 2 international organisations: the African Union and the European Union. National military manuals fell outside the scope of the research. It must be emphasised, however, that the number of positions is very small in comparison with the international community as a whole. Out of the 36 national positions analysed, only 9 mention direct participation in hostilities, which is exactly 25% of the total number.

Austria (2024) contends that "[c]ivilians who directly participate in hostilities lose their protection against attack. In the cyber context, direct participation in hostilities commences with the first cyber activity launched and continues throughout the period of intermittent activity, resulting in the individual being a lawful target for the entire period of cyber activities conducted."[87] Austria is the only state among those examined here to argue that direct participation lasts from the first act to the last, including intermittent periods. This results in the broader targetability of civilians participating in hostile cyber operations.

In contrast, the United Kingdom (2021) affirms that "[c]ivilians are protected from attack unless and for such time as they take a direct part in hostilities. To the extent that civilians carry out cyber operations in an armed conflict that amount to attacks, they would lose their protected status under IHL and, by taking a direct part in hostilities, become legitimate military targets."[88] Surprisingly, this formulation results in the narrowest possible scope of targetability for civilian hackers. It should be noted that this position does not fully align with the IRCR's IG,[89] and, when combined with the United Kingdom's position on attacks under IHL, suggests that a civilian only participates directly in hostilities if the cyber operation

---

86 The examined national positions can be found in English at the Cyber Law Toolkit, see https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions (accessed: 16.10.2024). Further positions can be found in the Nordic Journal of International Law's Volume 92 Issue 3. See: https://brill.com/view/journals/nord/92/3/nord.92.issue-3.xml (accessed: 16.10. 2024). The recently published position of Belgium can be accessed here: *The national position of Belgium on international law applicable to cyberspace – 2025*. Available from: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/National_position_BE_on_international_law_DEF_171025.pdf (accessed: 10.12.2025).

87 *Position Paper of the Republic of Austria: Cyber Activities and International Law*, April 2024, p. 18. Available from: 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 (accessed: 16.10.2024), p. 18.

88 *Policy paper. Application of international law to states' conduct in cyberspace: UK statement*, June 3, 2021. Available from: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/71358e6f-f834-4d09-88be-d5a13f8bf1df (accessed: 16.10.2024), para. 25. Please note, that this policy paper was published under the Johnson administration.

89 See Section II for detailed elaboration.

causes effects that are identical or similar to those of kinetic operations.[90] The traditional understanding of an attack under IHL encompasses acts that cause physical effects, namely death or injury to persons or damage or destruction of objects.[91] Because this excludes electronic data from the status of objects due to the physical nature of the damage,[92] cyber operations such as the one conducted by the Cyber Partisans of Belarus against the Belarusian railway system would not qualify as direct participation in hostilities. It is unclear whether this formulation was intentional on the part of the United Kingdom, but its consequences are clear.

France (2019), on the other hand, expressly states its position on what kinds of cyber operations the state deems to constitute direct participation. "A cyberoperation which is carried out to adversely affect the military operations or military capacity of a party to an armed conflict to the detriment of that party and to the advantage of an adversary, or which is likely to cause loss of human life, injury and civilian damage may be deemed a direct participation in hostilities."[93] Please note, that this formulation is significantly broader than that of the United Kingdom. According to this, not only attacks – i.e. operations that cause loss of human life, injury, damage or destruction to civilian objects – but other operations that create a military advantage for one side and/or an obstacle for the other will amount to DPH. France also gives examples of DPH activity in the cyberspace: (i) information gathering operations by cyber means for the specific purpose of a subsequent attack; (ii) installing malicious code; (iii) preparing a botnet for a DoS attack; and, finally, (iv) hostile software development.[94] It is important to note that France also highlights that targeting individuals participating in hostilities in the cyber realm is marginal because of the difficulties arising from target identification.[95] This appears to be a reference to the attribution problem in cyber operations.[96]

---

90 *Policy paper. Application of international law to states' conduct in cyberspace: UK statement.* June 3, 2021. Available from: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/71358e6f-f834-4d09-88be-d5a13f8bf1df (accessed: 16.10.2024), para. 24.

91 In the context of cyber operations, see M. Schmitt, *Tallinn Manual 2.0…*, p. 415, Rule 92; B. Kis Kelemen, *International armed conflicts in cyberspace,* "Intereulaweast" 2025, 1, p. 330.

92 B. Kis Kelemen, *Protection of (Personal) Data…*, pp. 7–9.

93 See the original French text here: *Droit international appliqué aux opérations dans le cyberespace*, 2019. Available from: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf (accessed: 16.10.2024), p. 15; for providing an English translation, I used the version published on the Cyber Law Toolkit see here: *National Position of France*, 2019. Available from: https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#cite_note-24 (accessed: 16.10.2024).

94 *Ibidem.*

95 *Ibidem*, p. 16.

96 K. Csillik, A. Hordós, *Zárva tartani Pandora szelencéjét: az erőszakos kiberműveletek betudásának kérdései*, "Katonai Jogi és Hadijogi Szemle" 2023, 3–4, pp. 6–51. J. Vastoupal, K. Uhlířová, *op. cit.*

 DOI: 10.7206/kp.2080-1084.860

Similarly, Germany (2021) first clarifies the preconditions for direct participation. For this purpose, the German national position uses the wording of the ICRC's IG and refers to the three cumulative criteria of direct participation: threshold of harm, direct causation and belligerent nexus. Germany also illustrates its position with examples: (i) electronic interference with military computer networks; (ii) wiretapping of the high command; or (iii) the transmission of information for an attack.[97] Once again, it needs to be highlighted, that this position creates a significantly broader group of direct participants than that of the United Kingdom, but it also seems to be broader than the position put forward by France, as it also includes wiretapping. It should also be noted that both France's and Germany's positions are more inclusive than the Tallinn Manual majority view, and that Germany not only uses the terminology of the IG but also the examples it provides.

Czechia and Sweden also refer to direct participation in hostilities in their respective national positions. These positions reaffirm the protected status of civilians unless, and for such time as, they directly participate in hostilities. Neither state provided further elaboration; however, in both cases, the following sentences stated that in cases of doubt, a person should be considered or presumed to be a civilian[98]. Although these are almost verbatim references to Article 50(1) of AP I[99], which is not necessarily equivalent to the presumption against direct participation, some positions in the international legal literature treat it as such. It remains unclear whether these states intended to formulate their position so as to express a presumption against direct participant status. The European Union, in its 2024 position, recalled that direct participation may make use of cyber means.[100] Finally, Colombia called for further legal analysis of whether involvement in planning

---

97 The Federal Government of Germany, *On the Application of International Law in Cyberspace. Position Paper*, 2021. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed: 16.10.2024), p. 8.

98 *Czech Republic: Position paper on the application of international law in cyberspace*, 2024. Available from: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf (accessed: 16.10.2024), para. 41; *Government Offices of Sweden: Position Paper on the Application of International Law in Cyberspace*, 2022. Available from: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf (accessed: 16.10.2024), p. 7.

99 See AP I Article 50(1) „A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian."

100 Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace* (18 November 2024) 15833/24. Available from: https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf (accessed: 26.10.2025), p. 7.

and executing cyber operations or activities would qualify as DPH.[101] Brazil did the same[102].

It is worth considering the difference of opinion in the national positions outlined above. What could explain the diverging positions? Could this reflect differing assessments of various issues in the cyber domain, or could these positions be the result of a hasty "codification" effort designed to produce a national position? In my opinion, all of the above plays a role in this outcome. It is clear that states have different agendas regarding the classification of certain cyber operations, depending on whether they are conducting offensive or defensive cyber operations. While the UK focuses on national interests in allowing for a more flexible régime for conducting offensive operations, France and Germany more clearly adopt the defender's position, under which a wider range of targets can be seen as protected from the harmful effects of hostilities. The consequent representation of these interests in national positions, however, sometimes seems to have unintended consequences, as the UK example clearly shows. This is something that could have been identified and corrected had more time been dedicated to developing the national position in question.

It is also noteworthy that only a quarter of the positions examined addressed direct participation in hostilities in connection with cyber operations, but it is even more striking that less than 20% of all states have issued a position at all on international law applicable to cyber operations. What might explain this silence? States might not issue statements because they do not regard international legal issues in this field as politically important, because they lack sufficient funding or capacity to finance international legal analysis of these issues, or because they are waiting for a significant historical event that would trigger a substantial response by other states, which could then be replicated without further consideration. Scholarship on reactive silence also identifies the need to avoid giving an already issued national position further credibility by responding, the need to avoid geopolitical tensions, and issues relating to the understanding of cyber operations and international law in connection with them, as possible reasons for states' silence.[103]

---

101 Cancillería, *Colombia's National Position on the application of international law in cyberspace*, 2025. Available from: https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf (accessed: 26.05.2025), p. 14.

102 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. A/76/136. 13 July 2021. p. 23.

103 D.B. Hollis, B. Sander, *International Law and Cyberspace: What Does State Silence Say?*, „Temple University Beasely School of Law. Legal Studies Research Paper" 2022, 22, p. 25.

 DOI: 10.7206/kp.2080-1084.860

In my opinion, with the exception of the first reason, all of them are plausible explanations for the lack of more national positions in the first place. At present, it is likely that all of the above reasons are present to some extent and in combination, explain the small number of states issuing individual position on this issue. International legal scholars therefore warn against inferring too much from silence. There are, however, at least two relatively uncontroversial consequences of such silence: (i) existing customary international law will likely remain unchanged due to the lack of unified state practice and opinio juris; and (ii) silence also allows for non-state actors to fill the void in identifying applicable norms in cyberspace. The Tallinn process and the work of the ICRC speak for themselves in this regard.[104] It is important to note, however, that Estonia, Japan, the NATO Cooperative Cyber Defence Centre of Excellence, and the University of Exeter jointly produced a handbook on the development of national positions, which might support states in their efforts in this endeavour.[105] Another aspect of this problem is the silence of states regarding already published national positions. The international legal literature has identified that states rarely react to each other's individual positions. However, this may not have legal significance, given that international law applies in cyberspace, meaning that existing customary international law still binds states even if they do not issue a position or react at all.[106]

Conclusions

Based on the above considerations, international law, including IHL, undoubtedly applies to cyber operations. This means that civilians participating in a conflict are bound by these norms. Civilians enjoy protection from the dangers of armed conflict unless, and for such time, as they directly participate in hostilities. Direct participation might occur where a civilian launches a cyber operation, for instance, by hacking a government system and deploying malicious software. IHL, however, is not clear on many issues surrounding this notion: namely, the precise scope of direct participation activities is still not settled, the temporal scope of DPH is especially contentious, and it is also uncertain whether there is a presumption against direct participant status. In these circumstances, international law needs to offer clearer answers, especially considering the frequency, ease, and potential deadly consequences of civilian participation in cyber conflicts, as illustrated by

104 D.B. Hollis, B. Sander, *op. cit.*, p. 26.

105 K. Mačák, T. Dias, Á. Kasper, *Handbook on Developing a National Position on International Law and Cyber Activities. A Practical Guide for States,* Exeter, 2025.

106 D.B. Hollis, B. Sander, *op. cit.*, pp. 24–25. D. Akande, A. Coco, T. de Souza Dias, *op. cit.*, p. 9.

examples from the Russo-Ukrainian armed conflict. International law can provide concrete answers if states agree on the applicable legal norms governing this dimension of hostile military operations.

When it comes to the national positions of states, a few specific conclusions can be drawn. First, it should be noted that only a handful of states and international organisations expressed their views on international law applicable to cyberspace (36). Second, only 25% of that number (9) – most of which were European states[107] – provided any insight into what they consider to be direct participation in hostilities in cyberspace. Third, given the varied positions among the small number of states expressing their views, no significant conclusions can be drawn from state practice and opinio juris formulated in the national positions of states at this point. Fourth, increased awareness is extremely important for states in this field, because of the potential trade-offs that any given position may entail for other issues. To illustrate this point, one may refer to the United Kingdom's restrictive position on direct participation. This largely stems from the position taken by the state on attacks in cyberspace. If a state wishes to limit what constitutes an attack, perhaps to potentially limit its own responsibility when it employs its cyber capabilities, it might need to accept a reduced targetability for direct participants. For instance, it could not target individuals participating in hostilities where their conduct is harmful to the adversary but does not reach the level of an attack under IHL. The same is true in reverse. France and Germany took an expansive view of the object status of electronic data.[108] This protective rule has the effect of reducing the protection of individuals potentially participating in hostilities.

Based on the above, states need to identify customary international law and create subsequent practice under the applicable treaties that acknowledges both state interests: limiting their own responsibility when it comes to cyber operations and creating a balanced category for direct (cyber) participants in hostilities. To be clear, this article does not argue for the creation of a new category of individuals under the law of armed conflict. On the contrary, it calls for the application of existing rules on DPH in a clearer and more foreseeable manner, which makes it possible for individuals to plan their behavior and understand the consequences of even a simple act of hacking.

---

107 Only European states engaged meaningfully with the issue.

108 The Federal Government of Germany, *On the Application of International Law in Cyberspace. Position Paper*, 2021 Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed: 16.10.2024), p. 8; *Droit international appliqué aux opérations dans le cyberespace*, 2019. Available from: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf (accessed: 16.10.2024), p. 15.

 DOI: 10.7206/kp.2080-1084.860

A possible solution to this problem, however unrealistic, is a large-scale diplomatic conference at which states could adopt an authentic interpretation of the existing treaties and, if they deem it fit, modify existing rules to better reflect cyber realities.

References

Akande D., Coco A., 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" 2022, 1.

Biggio G., *The Legal Status and Targetability of Hacker Groups in the Russia-Ukraine Cyber Conflict*, "Journal of International Humanitarian Legal Studies" 2024, 1, https://doi.org/10.1163/18781527-bja10078.

Boothby W., *And for Such Time as: The Time Dimension to Direct Participation in Hostilities*, "New York University Journal of International Law and Politics" 2010, 1.

Buchan R., Tsagourias N., *Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?*, „EJIL:Talk!" 9 March 2022. Available from: https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ (accessed: 15.10.2024).

Cancillería, Colombia's National Position on the application of international law in cyberspace, 2025. Available from: https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf (accessed: 26.05.2025).

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ed. Yves Sandoz et al, Geneva 1987.

Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace (18 November 2024) 15833/24. Available from: https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf (accessed: 26.05.2025).

Crawford E., *Identifying the Enemy. Civilian Participation in Armed Conflict*, Oxford 2015.

Csillik K., Hordós A., *Zárva tartani Pandora szelencéjét: az erőszakos kiberműveletek betudásának kérdései*, "Katonai Jogi és Hadijogi Szemle" 2023, 3–4.

Cyber Law Toolkit. Available from: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions (accessed: 16.10.2024).

Cyber Operations Tracker, *Council on Foreign Relations*. Available from: https://www.cfr.org/cyber-operations/ (accessed: 15.10.2024).

Czech Republic: Position paper on the application of international law in cyberspace, 2024. Available from: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf (accessed: 16.10.2024).

Dornbusch J., *Das Kampfführungsrecht im internationalen Cyberkrieg*, Köln 2018.

Droit international appliqué aux opérations dans le cyberespace, 2019. Available from: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf (accessed: 16.10.2024).

From where to where are cyber incidents most frequently initiated and received? (Bar Chart), „European Repository of Cyber Incidents". Available from: https://eurepoc.eu/dashboard/ (accessed: 15.12.2025).

Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field UNTS: 970

Geneva Convention for the amelioration of the condition of the wounded, sick and shipwrecked members of the armed forces at sea UNTS: 971.

Geneva Convention relative to the protection of civilian persons in time of war. UNTS: 973.

Geneva Convention relative to the treatment of prisoners of war. UNTS: 972.

Gisel L., Rodenhäuser T., Dörmann K., 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" 2020, 102, https://doi.org/10.1017/S1816383120000387

Government Offices of Sweden: Position Paper on the Application of International Law in Cyberspace, 2022. Available from: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf (accessed: 16.10.2024).

Hathaway O. A., Pe'er I., Vera C., *Crowdsourced war*, „New York University Law Review" 2025, 100.

Henckaerts J.M., Doswald-Beck L., *Customary International Humanitarian Law*. Volume I. Rules, Cambridge 2009.

Hoffmann T., *War or peace? – International legal issues concerning the use of force in the Russia–Ukraine conflict*, "Hungarian Journal of Legal Studies" 2022, 3, https://doi.org/10.1556/2052.2022.00419

Hollis D.B., Sander B., *International Law and Cyberspace: What Does State Silence Say?* „Temple University Beasely School of Law. Legal Studies Research Paper" 2022, 22.

How long does it take for the initiator of a cyber incident to be attributed? (Attribution speed), „European Repository of Cyber Incidents". Available from: https://eurepoc.eu/dashboard/ (accessed: 15.12.2025).

International humanitarian law and the challenges of contemporary armed conflicts report, "International Committee of the Red Cross", October 2015. Available from: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts (accessed: 15.10.2024).

Jones C., *Red Cross lays down hacktivism law as Ukraine war rages on*, "The Register" 4 October 2023. Available from: https://www.theregister.com/2023/10/04/red_cross_hacktivist_rules/ (accessed: 15.10.2024).

Kis Kelemen B., *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására*, Pécs 2023.

Kis Kelemen B., *Human Shielding, Subjective Intent, and Harm to the Enemy*, "Journal of Conflict & Security Law" 2020, 3. https://doi.org/10.1093/jcsl/kraa015.

Kis Kelemen B., *International armed conflicts in cyberspace*, "Intereulaweast" 2025, 1. https://doi.org/10.22598/iele.2025.12.1.12

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

Kiss M., *A kiberműveletek és a jus ad bellum kapcsolata*, „Jura" 2022, 3.

Kiss M., *Kiberműveletek a beavatkozás tilalma mint nemzetközi jogi alapelv tükrében*, "Állam- és Jogtudomány" 2023, 4. https://doi.org/10.51783/ajt.2023.4.05

Kittichaisaree K., *Public International Law of Cyberspace*, Cham 2017.

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

Ma E.H., *Autonomous Weapons Systems under International Law*, "New York University Law Review" 2020, 5.

Mačák K., Dias T., Kasper Á., Handbook on Developing a National Position on International Law and Cyber Activities. A Practical Guide for States, Exeter 2025.

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" 2019, 2.

Melzer N., In*terpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva 2009.

Melzer N., *Targeted Killing in International Law*, Oxford 2008.

National Position of France, 2019. Available from: https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#cite_note-24 (accessed: 16.10.2024).

Nordic Journal of International Law's Volume 92 Issue 3. https://brill.com/view/journals/nord/92/3/nord.92.issue-3.xml (accessed: 16.10.2024).

Parks W.H., *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate*, No Expertise, and Legally Incorrect "New York University Journal of International Law and Politics" 2010, 1.

Policy paper. Application of international law to states' conduct in cyberspace: UK statement, June 3, 2021. Available from: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/71358e6f-f834-4d09-88be-d5a13f8bf1df (accessed: 16.10.2024).

Pomson O., *Methodology of identifying customary international law applicable to cyber activities*, "Leiden Journal of International Law" 2023, 4. https://doi.org/10.1017/S0922156523000390

Position Paper of the Republic of Austria: Cyber Activities and International Law, April 2024. Available from: 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 access: 16 October 2024).

Rodenhäuser T., Vignati M., *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them*, "Humanitarian Law & Policy" 4 October 2023. Available from: https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ (accessed: 15.10.2024).

Saballa J., *Anduril Introduces Bolt-M Autonomous Attack Drone*, "The Defense Post" 11 October 2024. Available from: https://thedefensepost.com/2024/10/11/anduril-bolt-attack-drone/ (accessed: 15.10.2024).

Schmitt M., *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, "Just Security" 9 February 2017. Available from: https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ (accessed: 16.10.2024).

Schubert B., *Az fegyverrendszerekkel szemben támasztott követelmények a humanitárius nemzetközi jog tükrében*, "Honvédségi Szemle" 2022, 3. https://doi.org/10.35926/HSZ.2022.3.2

Stuxnet, "Britannica". Available from: https://www.britannica.com/technology/Stuxnet (accessed: 15.10.2024).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, ed. M. Schmitt Oxford 2017.

The Federal Government of Germany, On the Application of International Law in Cyberspace. Position Paper, 2021. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed: 16.10.2024).

The national position of Belgium on international law applicable to cyberspace – 2025. Available from: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/National_position_BE_on_international_law_DEF_171025.pdf (accessed: 10.10.2025).

Vastoupal J., Uhlířová K., *Of Hackers and Privateers: The Possible Evolution of Cyber Attribution*, „Masaryk University Journal of Law and Technology" 2024, 2. https://doi.org/10.5817/mujlt2024-2-2.

Watkin K., *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, "New York University Journal of International Law and Politics" 2010, 1.