Научная статья / Research Article
https://doi.org/10.17323/jil.2025.27025

Legal qualification of IT specialists from the international humanitarian law perspective

A. Santalova*

HSE University, Moscow, Russia

asantalova@hse.ru
ORCID: 0009-0008-1335-2247

Abstract

Ever-evolving technologies significantly affect modern warfare. The use of information and communication technologies (hereinafter — ICTs) for malicious purposes in armed conflicts is increasing significantly. Moreover, there are new potential armed conflict participants, such as IT specialists. The question arises: how participation of IT specialists in armed conflicts may be qualified in accordance with the existing international humanitarian law (hereinafter — IHL)? Are they still civilians protected from attacks, or do they lose this protection as legitimate combatants? This situation highlights new legal challenges as the main rules of IHL were drafted in a very different technological age. The present research focuses on analysing the adequacy of application of the IHL in assessing the status of IT specialists in modern armed conflicts. National positions of more than 30 States with regard to the relevant problem and academic approaches were examined. The author concludes that the terminological limits of IHL make it very difficult to classify IT specialists as a specific category of persons within armed conflict. The category of direct participation of hostilities sometimes may be the most perspective, however, it has its own ambiguities. IHL norms do not take into account new capacities such as the remote location of IT specialists, the anonymity and secrecy inherent in their activities, etc. In addition, some IHL standards demonstrate their practical inapplicability to real-life situations involving the malicious use of ICTs. Nevertheless, the mix of potential statuses of IT specialists can be very dangerous for the protection of both armed conflict participants and civilians in general. Therefore, in accordance with the operating hypothesis, it is demonstrated that IHL as a regulator is poorly adequate in its application to ICTs due to corresponding restrictions of terms used, which are not adjusted to non-traditional armed conflicts. *De lege ferenda*, adjusting the interpretation of direct participation in hostilities category as most suitable to IT specialists in a cautious manner might be a possible solution.

Key words: IT specialists, malicious use of information and communication technologies, armed conflict, direct participation in hostilities, *levée en masse*, international humanitarian law

Citation: Santalova A. Legal qualification of IT specialists from the international humanitarian law perspective. *HSE University Journal of International Law*. 2025. Vol. 3. No 1. P. 46–68.

[*] **Anastasia V. Santalova** — Research intern, International Justice Laboratory.

Правовая квалификация IT-специалистов в соответствии с международным гуманитарным правом

А. В. Санталова[*]

Национальный исследовательский университет

«Высшая школа экономики», Москва, Россия

asantalova@hse.ru

ORCID: 0009-0008-1335-2247

Аннотация

Развивающиеся технологии ощутимо влияют на ведение войн, и количество случаев злонамеренного использования информационно-коммуникационных технологий (далее — ИКТ) в современных вооруженных конфликтах растет. Более того, появляются новые потенциальные участники вооруженных конфликтов — IT-специалисты. Но как квалифицировать участие IT-специалистов в вооруженных конфликтах в соответствии с нормами существующего международного гуманитарного права (далее — МГП)? Являются ли они гражданскими лицами, защищенными от нападений, или же комбатантами, утратившими такую защиту? Подобная ситуация порождает новые правовые проблемы, поскольку основные нормы МГП были разработаны во времена, когда уровень технологического развития в мире был совершенно иным. Настоящее исследование посвящено анализу адекватности применения МГП при оценке статуса IT-специалистов в современных вооруженных конфликтах. В рамках исследования данной проблемы были изучены национальные позиции более 30 государств и существующие научные подходы. Автор приходит к выводу, что в силу терминологических ограничений МГП отнести IT-специалистов к той или иной категории лиц в рамках вооруженного конфликта очень сложно. Наиболее состоятельным решением проблемы видится их отнесение к категории непосредственных участников боевых действий, однако и этот вариант сопряжен с определенными сложностями. Нормы МГП не учитывают такие особенности работы современных IT-специалистов как удаленное расположение, анонимность, секретность и т. д. Более того, некоторые нормы МГП оказываются практически не применимыми к реальным ситуациям, связанным со злонамеренным использованием ИКТ. Тем не менее смешение потенциальных статусов

IT-специалистов может быть весьма опасным для защиты как участников вооруженных конфликтов, так и гражданских лиц в целом. В соответствии с рабочей гипотезой продемонстрировано, что на сегодняшний день МГП не может обеспечить адекватное регулирование ИКТ ввиду терминологических ограничений, поскольку его понятийный аппарат не приспособлен к нетрадиционным вооруженным конфликтам. Возможным решением *de lege ferenda* может стать корректировка толкования категории «непосредственное участие в боевых действиях» как наиболее подходящей для IT-специалистов. Однако это необходимо делать с осторожностью во избежание слишком широкого толкования.

Ключевые слова: IT-специалисты, злонамеренное использование информационно-коммуникационных технологий, вооруженный конфликт, непосредственное участие в боевых действиях, *levée en masse*, международное гуманитарное право

Для цитирования: Санталова А. В. Правовая квалификация IT-специалистов в соответствии с международным гуманитарным правом. *Журнал ВШЭ по международному праву / HSE University Journal of International Law*. 2025. Том 3. № 1. С. 46–68.

[*]**Анастасия Вадимовна Санталова** — стажер-исследователь, Лаборатория международного правосудия.

Cyber warfare does not play out in the abstract.
Rather, it can have a profound impact on people's lives.

K. Khan, ICC chief prosecutor

Introduction

Nowadays the world continues to be plagued by armed conflicts. 27 conflicts are still ongoing.[1] In addition to traditional military methods, States adhere to the malicious use of ICTs both in the course of ongoing armed conflicts or in peacetime. But how participation of IT specialists in armed conflicts may be qualified under existing IHL? Are they still civilians protected from attacks or lawful combatants losing such a protection? Even though relatively few States have publicly admitted malicious use of ICTs' for military purposes, a growing number are developing military cyber capacities. Therefore, according to the International Committee of the Red Cross (hereinafter — ICRC), their use in future is expected to be expanded (ICRC, 2020, p. 483). In August 2023, the chief prosecutor of the International Criminal Court (hereinafter — ICC),

[1] Council on Foreign Relations. *Global Conflict Tracker*. https://www.cfr.org/global-conflict-tracker.

K. Khan, claimed that the Court was ready to prosecute “cyberattacks” as international crimes pursuant to the Rome Statute.[2]

The whole situation is very challenging. IHL as a regulator faces significant complexities because at the time when its main rules were drafted the technological state of the world was different. Thus, there are no special IHL provisions governing malicious use of ICTs and especially the status of IT specialists. For the purpose of this article, this notion embraces numerous technical professionals skilled in ICTs who are involved in a variety of relevant activities (Turns, 2012, pp. 289, 295; ICRC, 2013, p. 3). The existing consensus among States has developed at a high level of abstraction: it hardly exceeds the extension of general IHL scope to the cyber sphere. As a result, the international legal assessment of the relevant cases is highly ambiguous (Rusinova, 2022, p. 49). The scholarship on the topic is also less developed.

However, this uncertainty affects the participants of such cyber activities, their potential direct victims and civilians in general. They all need to be protected to the maximum extent possible by existing IHL and be aware of the permissible limits of their actions and their possible consequences in order to minimise the risks inherent in such conflicts.

Under these circumstances, the following research question arises: to what extent does the current IHL adequately address the issue of the legal status of IT specialists? The operating hypothesis is that IHL is poorly adequate as a regulator in this regard due to corresponding restrictions of terms used, which are not adjusted to non-traditional armed conflicts’ participants.

The present research is distinguished by the methods chosen. Thus, a critical analysis is used to explain the terminological limitations of the IHL terms; an interdisciplinary approach — to assess political rationales behind some choices. The research is based on analysis of more than 30 positions of the national States on the issue.

1. Applicability of IHL and law of targeting to the cyber sphere

The research is based on the premise that IHL is generally applicable to the malicious use of ICTs. At least 28 States made the relevant statements.[3] At the

---

[2] Khan, K. (20 August 2023) Technology will not exceed our humanity. *Digital Front Lines*. URL: digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.

[3] See the examples: International humanitarian law (*jus in bello*). In Mačák, K., Minárik, T., Jančárková, T. (Eds). *Cyber Law Toolkit (2019-)*.
URL: https://cyberlaw.ccdcoe.org/wiki/International_humanitarian_law_(jus_in_bello). See also:, Federal Department of Foreign Affairs (May 2021). *Switzerland's position paper on the application of international law in cyberspace*; United Kingdom Foreign, Commonwealth & Development Office (3 June 2021). *Application of international law to states' conduct in cyberspace: UK statement*; Italian Ministry for Foreign Affairs and International Cooperation Italy (2021). *Italian position paper on "International law and cyberspace"*, p. 3; Ministry of Defense of France (9 September 2019).

same time some States oppose its applicability as it may legitimise militarisation of cyberspace (Rusinova, 2022, p. 47).[4] According to the prevailing approaches, cyber activities together with traditional kinetic military actions may be qualified as actions "in the context of an armed conflict" (Schmitt, 2013; Roscini, 2014, p. 122) provided that "belligerent nexus" (Melzer, 2009, p. 58)[5] is present. The cases where ICTs are used autonomously are more complicated and controversial. Besides, in the most challenging situations physical damage typical of traditional kinetic weapons is absent (Droege, 2012; Rochini, 2014, p. 135).

Although cyber capabilities may generally be regarded as means and methods of warfare,[6] attaining an "attack"[7] threshold, which is higher than a "military operation",[8] can be very complicated due to the terminological limitations of IHL. The main precondition is the absence of typical violent consequences (Schmitt, 2011, p. 6; Dinstein, 2013, p. 284). Nevertheless, these concepts are sometimes manipulated. For instance, Tallinn Manual drafting experts (Schmitt, 2013; Schmitt, 2017), the ICRC,[9] and many scholars (Rochini, 2014; Droege, 2012; Gisel, Rodenhäuser, & Dörmann, 2020) have used the terminology of "cyber operation"' and "cyber-attack" for the malicious use of ICTs in general, even before the applicability of IHL to these acts has been established, thus encompassing both legitimate and illegitimate acts. This may cause confusion with the IHL categories of "military operations" and "attacks".

International Law Applied to Operations in Cyberspace, p. 6; Ministry of Foreign Affairs of Poland (29 December 2022). *The Republic of Poland's position on the application of international law in cyberspace*, p. 1; Ministerio de Relaciones Exteriores y Culto (21 July 2023). *Costa Rica's Position on the Application of International Law in Cyberspace*, p. 3; UNODA (3 March 2023). *Pakistan's Position on the Application of International Law in Cyberspace*, p. 6–8; African Union Peace and Security Council (29 January 2024). *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, p. 1.

4 Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (23 June 2024); Ministry of Foreign Affairs of the Russian Federation (29 June 2017). *Answer by A.V. Krutskikh, Special Representative of the President of the Russian Federation on International Cooperation in the Field of Information Security, to a question by the TASS news agency on the status of international dialogue in this sphere*; Korzak, E. (2017). UN GGE on cybersecurity: the end of an era? *The Diplomat*, 31; Open-Ended Working Group (OEWG). (2019). *First substantive session*; Open-Ended Working Group (OEWG). (2020). Second substantive session.

5 ICRC (2016). *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*. Cambridge University Press.

6 *Legality of the Threat or Use of Nuclear Weapons* [1996] ICJ Advisory Opinion, p. 226; ICRC Report on International Humanitarian Law and the challenges of contemporary armed conflicts (28 November – 1 December 2011). *31st International Conference of the Red Cross and Red Crescent*, Geneva, Switzerland.

7 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), 1125 UNTS 3, Article 49(1).

8 AP I, Article 48.

9 See, for example, the ICRC report on cyber operations. (2019). *Security, Privacy & Tech Inquiries*.

On the other hand, the UN institutions[10] have chosen a more neutral wording — "malicious use of ICTs". What is important, established IHL principles may regulate cyber acts attaining the needed thresholds.[11] However, their application may still be complicated given the specifics of the cyber realm, for instance, the interconnectedness of computer systems and the prevalence of dual-use objects (Geiß & Lahmann, 2012, p. 14). This is particularly relevant for complying with the principle of distinction. The possibility to qualify data as a "civilian object",[12] which may trigger corresponding responsibilities for potential attackers, still raises heated debates (Gisel, Rodenhäuser, & Dörmann, 2020, pp. 317–318; Rochini, 2014, p. 179).

2. Legal qualification of IT specialists and rules applicable to them under IHL

"IT specialists" embrace a wide range of ICTs professionals. Hence, it is not correct to state that this category of persons as such loses the privileges of civilians and becomes susceptible to attack. Besides, such an indiscriminate classification would expose a part of these professionals and the civilian population as a whole to unwarranted risk. Many types of malicious use of ICTs do not attain the armed conflict threshold, therefore, IHL is not applicable. Even if the armed conflict is in place, many IT specialists are likely to be considered civilians who continue to be under the IHL protection from direct attack. At the same time, they may still be targeted by law enforcement and potential criminal prosecution if their actions breach other legal rules.[13] This scenario changes if IT specialists engage directly in hostilities through cyber activities attaining a minimal gravity threshold and supporting one of the conflict's parties. Thus, it is necessary to analyse how exactly IT specialists may be qualified under IHL and how IHL rules may apply to them.

2.1. International armed conflict

In an international armed conflict (hereinafter — IAC), combatants and civilians are traditionally distinguished. Combatants are defined by the ICRC as "persons with a right to directly participate in hostilities between States".[14] These persons

---

10 Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021) A/76/135; Final report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (10 March 2021) A/AC.290/2021/CRP.2.

11 GGE Report, 71(f).

12 AP I, Article 52.

13 ICRC. Cyberwarfare, p. 3–4.

14 Combatants. In ICRC. *How does law protect in war? Online casebook*. URL: https://casebook.icrc.org/a_to_z/glossary/combatants.

comprise, firstly, members of regular "armed forces of a Party to a conflict"[15] and, secondly, members of irregular armed forces (Rusinova, 2015, p. 175) such as "militias and… other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict".[16] According to Article 4(A)(2) of the Third Geneva Convention (hereinafter — GC III), four criteria must be met: (1) having a responsible command;[17] (2) having "a fixed distinctive sign recognizable at a distance";[18] (3) "carrying arms openly";[19] and (4) complying with "the laws and customs of war".[20] Y. Dinstein also specifies that chapeau of this Article provides two other criteria: being "organized"[21] (Dinstein, 2022, p. 36) and "belonging to a Party to the conflict",[22] meaning, according to the ICRC Commentary, a "*de facto* relationship between the resistance organization and [the party] which is in a state of war" (Pictet, 1960, p. 57). Thus, the group must "in fact fight on behalf of that Party" and the party must "accept both the fighting role of the group and the fact that the fighting is done on its behalf" either expressly or tacitly (ICRC, 2021, para. 1005–1007). Meanwhile, the term "armed" implies the presence of violence.

IT specialists may be embedded explicitly within the regular armed forces in the manner of "military cyber units",[23] and, consequently, qualified as combatants. If such specialists have a weaker connection to a conflict's party, they may constitute irregular armed forces, provided the abovementioned criteria are met.

In the cyber realm, however, it is debatable whether IT specialists have to "carr[y] arms openly".[24] Even though it is admitted, it may be practically impossible. Computers and software traditionally used by IT specialists may hardly be regarded as weapons and, therefore, they cannot "carry arms openly". Even though they may, as weapons may be defined as any tool which causes damage,[25] the practical issues rise especially with regard to malware and code (Buchan & Tsagourias, 2022). To avoid physical impossibility this requirement may be interpreted as obliging IT specialists to fully disclose their code but it would also be unrealistic as the main upside of cyber acts is their unexpected

---

15 Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention) (12 August 1949) 75 UNTS 135, Article 4(A)(1).
16 GC III. Article 4(A)(2).
17 Ibid. Article 4(A)(2)(a-d).
18 Ibid.
19 Ibid.
20 Ibid. Article 4(A)(2)(a-d).
21 Ibid. Article 4(A)(2).
22 Ibid.
23 In Mačák, K., Minárik, T., Jančárková, T. (Eds). *Cyber Law Toolkit (2019-)*. URL: https://cyberlaw.ccdcoe.org/wiki/Combatancy.
24 Ibid.
25 ICJ. *Nuclear Weapons*, para. 39.

nature (Biggio, 2024, p. 161). Potential exception for situations when "combatant cannot so distinguish himself"[26] contained in Article 44(3) of Additional Protocol I (hereinafter — AP I) and valid for its parties[27] (Mačak & Schmitt, 2018, p. 359) is also hardly applicable as actions in the cyber realm are not "visible to the adversary" and "each military engagement"[28] is conducted anonymously (Biggio, 2014, p. 162). Another proposal was to conduct acts of malicious ICTs use only from designated IP addresses (Dinniss, 2012, p. 146). Nevertheless, "requiring a computer to be marked as a military computer is tantamount to placing a target on any system to which it is connected" (Dinniss, 2013, p. 257). Besides, secrecy and anonymity are inherent characteristics of IT specialists' actions.

The requirement of "a fixed distinctive sign recognizable at a distance" is also problematic as IT specialists tend to work on their computers inside buildings. However, it is rigid in temporal and geographical closeness to the combat zone, but may be interpreted less strictly in cases where combatants act in locations beyond the hostilities area or outside operational hours (Pfanner, 2004, p. 101). Thus, in the cyber context, this criterion must also be fulfilled if the actual battlefield is rather close, however, IT specialists tend to work remotely (Dinniss, 2012, p. 148). On the contrary, the experts of the Tallinn Manual believe that "there is no basis for deviating from this general requirement" (Schmitt, 2017, p. 405) and it is generally attained by wearing a uniform. Thus, the issue of differentiation between cyber combatants and ordinary people which is heated by the possibility of computers' dual use is generally apparent (D'Urso, 2015).

Another approach includes the deprivation of combatant status in case of using botnets,[29] IP address spoofing[30] or other means that render civilians and combatants in the cyber sphere indistinguishable (Buchan, 2016, p. 748). However, such methods not infringing IHL may be considered "ruses of war",[31] authorised by customary rule reflected in AP I, Article 37(2) (Henckaerts, Doswald-Beck, Alvermann, Dörmann, & Rolle, 2006, Rule 57). The requirement of distinctive sign might be met if cyber activities "are not conducted by feigning protected, non-combatant status within the meaning of the prohibition of

---

26 AP I. Article 44(3).

27 This exception was objected by nonparties and has not yet become customary. See US Department of Defence. (2016). *Law of War Manual*, p. 119; Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts (1974–1977) Geneva, vol. VI, p. 121.

28 AP I. Article 44(3)(a)(b).

29 CISA. (1 February 2021). *Understanding denial-of-service attacks*. URL: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

30 Kaspersky. *IP spoofing: how it works and how to prevent it*. URL: https://www.kaspersky.com/resource-center/threats/ip-spoofing.

31 AP I. Article 37(2).

perfidy"[32] (Melzer, 2011, p. 34). Customary (Henckaerts et al., 2006, Rule 65) provision in AP I Article 37(1) "prohibit[s] to kill, injure or capture an adversary by resort to perfidy"[33] *inter alia* by "feigning of civilian, non-combatant status".[34] Nevertheless, most acts of malicious use of ICTs do not result in such violent consequences. An analogy may be drawn with traditional combatants, who, in line with the ICRC interpretation, are not expected to carry their weapons "at belt or shoulder rather than in a pocket or under a coat" (Pictet, 1960, p. 61), but be recognisable as combatants. Thus, IT specialists may also try to avoid detection, but cannot operate, for instance, from civilian objects such as schools or hospitals (Waters, 2014, p. 784). The disclosure of their geographic location may be a potential decision. Besides, labelling of attacks with an "encrypted signature" may be used.[35] It should be kept hidden from incidental scrutiny, probably with a decryption key that is familiar to the offender or neutral actor that reveals who is the author of the attack.[36] Thus, it may help to avoid cyber perfidy (Schmitt, 2013, Rule 60) carried out by non-authorised actors pretending to have a legitimate military status under false pretexts.[37]

As for another criteria, IT specialists may act individually or without a centralised command. They may not be acquainted with IHL rules. Virtual interaction may also impede the consistency with such rules due to the lack of the enforcement mechanisms (Schmitt, 2012, p. 462). Finally, their applicability also depends on a conflict's and its participants' qualification.

Another category of persons which may be regarded as combatants are civilians participating in *levée en masse* (Rusinova, 2015, p. 181). This category includes "inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, lacking time to form themselves into regular armed units".[38] They also must openly bear arms and honor war laws and customs.[39]

Tallinn Manual experts were not unanimous on the relevance of this category in cyber context. While cyber *levée en masse* is possible in theory, it seems to be implausible in the cyber realm in practice (Waters, 2014, p. 780). Others nonetheless see it as practically relevant (Wallace & Reeves, 2013, p. 648). It is sometimes regarded as even more applicable to malicious use of ICTs than to

---

32 AP I. Article 37(1)(c).
33 AP I. Article 37(1).
34 Ibid. Article 37(1)(c).
35 Kostadinov, D. (2014). *Jus in cyber bello: how the law of armed conflict regulates cyber attacks. Part II*. Infosec Resources. URL: https://resources.infosecinstitute.com/topic/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part-ii/.
36 Ibid.
37 Kostadinov, D. *Jus in cyber bello*.
38 GC III. Article 4(A)(6).
39 Ibid.

kinetic operations (Waters, 2014, p. 785). Anyway, there are some possible challenges.

Firstly, a restricted number of potential participants. “It is unclear whether *levée en masse* can be composed solely of a significant portion of the cyber-capable members of the population” (Schmitt, 2013) since usually it is composed of the majority of the population. Not many people are competent to take part in cyber warfare. At the same time, not all traditional *levée en masse* participants are equally qualified. Some actors can reveal vulnerabilities in their adversary's target systems, some may devise malware to take advantage of those vulnerabilities, and others may participate in “denial of service attacks or defences” (Schmitt, 2012, p. 256). Besides, some types of malicious use of ICTs are connected with social networks, subsequent propaganda and mobilisation of population to fight and its coordination. These tasks can be performed by a wider number of people. Besides, the level of cyber awareness and competence is increasing (Waters, 2014, p. 781).

Secondly, it is not clear whether *levée en masse* may be applied in response to cyber or kinetic activities. Many experts see the necessity of the kinetic ones. However, the “approach of the enemy” seems to be possible in a cyber realm too. Moreover, kinetic operations and malicious use of ICTs often complement each other (Waters, 2014, p. 781). Melzer even considered that while this category “has become ever less relevant in traditional warfare”, it may be “of practical importance in cyberwarfare”, where “territory is neither invaded nor occupied, which may significantly prolong the period during which a *levée en masse* can operate” (Melzer, 2011, p. 34).

Thirdly, it is ambiguous whether this cyber “resistance” may include attacks behind adversary front lines. Corresponding limitation might be harmful and impractical for *levée en masse* participants in the cyber sphere due to significant decrease of the defense possibility. Finally, the abovementioned challenge of “carrying arms openly” also arises (Waters, 2014, p. 783).

If such a rebellion takes place on the occupied territory, its members must correspond to the resistance movement’s members criteria, such as having a responsible command and an internal disciplinary system consistent with international law rules governing armed conflict, as it is clarified by the ICRC (Pictet, 1960, p. 59). In such a case the situation is more complex as IT specialists may act autonomously or chaotically without a disciplinary system or a centralised command. Compliance with IHL rules is also a relevant issue.

Thus, while in some cases IT specialists may be regarded as combatants, compliance with traditional requirements may often be practically impossible. As for specific rights and protection given by IHL, combatants have a “privilege” to

"participate directly in hostilities"[40] (Henckaerts et al., 2006, Rule 3) and have corresponding combatant immunity, which prevents their prosecution for these actions if they are consistent with IHL limits and do not amount to war crimes.[41] However, they lose protection from attacks.[42] Combatants are entitled to a prisoner of war (hereinafter — POW) status[43] and corresponding rights.[44] They are protected once they no longer take part in hostilities, if they have been captured in the adversary's power — in POW status, "wounded, sick and shipwrecked"[45] or "parachuting from an aircraft in distress".[46] These conditions, however, are losing their relevance in the cyber sphere. Protection also spreads against "some means and methods of warfare"[47] even during taking part in hostilities.[48] Assessing the threats to IT specialists' lives arising from the combatant status in exchange for corresponding "privileges" and the difficulties in their applicability to the cyber sphere, it may be concluded that IT specialists should be qualified as such in very limited cases.

If IT specialists are not incorporated or assimilated in abovementioned ways, they retain their status as civilians.[49] The definition of civilian persons is provided by the customary (Henckaerts et al., Rule 5) Article 50 of AP I as any person not falling under the scope of GC III Article 4(A)(1),(2),(3),(6)[50] and AP I Article 43.[51] Moreover, this notion encompasses all the persons "who accompany the armed forces without actually being members thereof",[52] members of the crews of civil aviation, merchant ships and internees belonging to armed forces of the occupied State. Furthermore, persons who take or have taken direct part in military actions without having the combatants' status also belong to civilians (Rusinova, 2015, p. 185). AP I specifies that "in case of doubt whether a person is a civilian, that person shall be considered to be a civilian".[53]

---

40 AP I. Article 43(2); Henckaerts et al. Customary IHL, rule 3.

41 Immunities. In ICRC. *How does law protect in war? Online casebook*. URL: https://casebook.icrc.org/a_to_z/glossary/immunities.

42 Principle of distinction. In ICRC. *How does law protect in war? Online casebook*. URL: https://casebook.icrc.org/law/principle-distinction.

43 GC III. Article 4.

44 Ibid.

45 ICRC. Principle of distinction; Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) (12 August 1949), 75 UNTS 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention) (12 August 1949), 75 UNTS 85; GC III; AP I.

46 Ibid.

47 ICRC, Principle of distinction; AP I.

48 Ibid.

49 Combatancy. In Mačák, K., Minárik, T., Jančárková, T. (Eds). *Cyber Law Toolkit (2019-)*. URL: https://cyberlaw.ccdcoe.org/wiki/Combatancy.

50 GC III. Article 4(A)(1), (2), (3), (6).

51 AP I. Article 43.

52 GC III. Article 4(A)(4).

53 AP I. Article 50.

Civilians are protected from attacks unless and for such a period they "directly participate in hostilities" (Henckaerts et al., 2006, Rule 6). They are also protected "in the hands of the enemy"[54] (e. g. "against arbitrary treatment",[55] under the "special rules on occupied territory"[56] and "against the effects of hostilities"[57]) (Henckaerts et al., 2006, Rule 6). However, remaining protected from attack, they cannot directly participate in hostilities, enjoy POW status[58] and combatant immunity. The protection "in the hands of the enemy"[59] and "against the effects of hostilities"[60] is also applicable to them. In many cases IT specialists may indeed be qualified as civilians. However, sometimes the lack of international responsibility may be critical given technological advances allowing it to remotely inflict far more damage than soldiers do on the battlefield.

2.2. Non-international armed conflict

Moving to a non-international armed conflict (hereinafter — NIAC), combatants and civilians are not defined in the IHL sources in this field. The States' position here is unsettled, therefore, the formation of an international custom still seems to be impossible. The most applicable approach is partially similar to the one in an IAC. Thus, "civilians" as those not related to parties of a conflict are distinguished from "organised armed groups" which are "under a command responsible to th[e] Party [to a conflict] for the conduct of its subordinates"[61] (Henckaerts et al., 2006, Rule 4) and "subject to an internal disciplinary system"[62] consistent with international law rules governing armed conflict.[63] This interpretation of an organised armed group in the NIAC is exercised by analogy with the IAC, thereby filling in the gaps of the NIAC law (Rusinova, 2015, p. 201). The membership in such groups is determined pursuant to a functional approach where the determinant shifts from the "direct participation in hostilities" (hereinafter — DPH) to the possession of a military function by the individual (Rusinova, 2015, p. 194, 202). The status of those armed group members who do not meet the above criteria or those who act independently ought to be assessed from the standpoint of DPH.

54 Ibid. GC IV; AP I; ICRC, Principle of distinction.
55 Ibid.
56 Ibid.
57 Ibid.
58 A special attention should be given to civilians "accompany[ing] armed forces without actually being members thereof" as they are entitled to POW status. GC III. Article 4(A)(4).
59 ICRC, Principle of distinction.
60 Ibid.
61 AP I. Article 43(1).
62 Ibid.
63 Ibid.

The complexity of qualification of IT specialists as organised armed groups is the following. IT specialists often operate autonomously. The number of such actors and their activities usually do not result in the fulfilment of the "organised" group threshold (Schmitt, 2012, p. 463). It is clarified that "even small groups of hackers are unlikely to meet the requirement of organization" (Schmitt, 2017, Rule 83). The problems of responsible command and internal disciplinary systems were mentioned before. Even though the group works cooperatively and has a governance unit coordinating its operations, for example, by distributing certain cyber targets among its members, sharing specific tools or vulnerability evaluations with each other, and conducting cyber harm reviews to identify the need for a "reattack", there may be specific difficulties. Although the group might be organised even without physical interactions, their absence may demonstrate the lack of means to enforce consistency with the rules of armed conflict. It is ambiguous whether this would be an obstacle to qualification of such a cyber group as "organised" within the IHL approaches to NIAC members. Traditionally it is, while given changing methods and actors of warfare, it should not be, according to the Tallinn Manual (Schmitt, 2017, Rule 83).

Conventionally, the protection during NIAC is not status-based but conduct-based[64] (Sassoli & Bouvier, p. 307). Nevertheless, IT specialists qualified as members of organised armed groups lose their protection not only during the DPH, but also until they are in the power of the adversary or are somehow *hors de combat*. Thus, by analogy with IAC, they can participate directly in hostilities but, subsequently, they lose the protection from attacks. Some experts and States believe that they can be detained because they belong to the enemy (as POWs in IAC, although this status is absent in NIAC along with combatant immunity) and enjoy minimal protection (Melzer, 2009, p. 84). The use of certain weapons is also prohibited.[65] Thus, such persons have similar disadvantages as combatants in IAC, but their privileges are smaller (Rusinova, 2015, p. 201). This also questions the qualification of numerous IT specialists.

If IT specialists do not fall within this category they may be qualified as civilians and enjoy "general protection against the dangers arising from military operations".[66] They are protected against attacks "unless and for such time as they take a direct part in hostilities".[67]

---

64 Non-international armed conflict. In ICRC. *How does law protect in war? Online casebook*. URL: https://casebook.icrc.org/law/non-international-armed-conflict.

65 Ibid.

66 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (8 June 1977), 1125 UNTS 609, Article 13(1).

67 Ibid. Article 13(3).

2.3. Direct participation in hostilities

The complex category of DPH is applicable to both IAC and NIAC. Modern armed conflicts tend to involve more civilians in military actions (Rusinova, 2015, p. 202). For instance, armed forces, especially of Western States, often outsource the activities of technical specialists to civilians (Turns, 2012, p. 279). Due to this "civilianisation", the DPH concept seems to be increasingly relevant and, at first glance, the most appropriate for the qualification of IT specialists in armed conflicts. The rule prescribing that civilians lose their protection from attack while "directly participating in hostilities" is manifested itself *inter alia* in common Article 3(1) of Geneva Conventions[68] and both AP I[69] and Additional Protocol II (hereinafter — AP II).[70] ICRC recognised this rule as customary in both IAC and NIAC (Henckaerts et al., 2006, pp. 25–31). This category should be interpreted restrictively, namely, as applicable to specific actions. In case there are doubts regarding the qualification of such individuals, in the ICRC view, they must be interpreted in favour of the civilian's status (Rusinova, 2015, c. 201–202; Pilloud, Sandoz, Swinarski, & Zimmermann, 1987, p. 1453).

Nevertheless, the issue of DPH has various limitations. It seems to be one of the vaguest in IHL and should be further detailed. Firstly, there is no exact definition of DPH (Henckaerts et al., 2006, p. 28). However, the lack of clearly delineated and understandable parameters[71] can lead to very dangerous consequences,[72] so they must be unambiguously defined. The approach identifying concrete acts encompassed and not encompassed by DPH does not solve the problem of "grey zone" (controversial acts) (Cassese, 2007, pp. 339–345) and cannot envisage all possible acts due to the specificity of each separate conflict. Therefore, common criteria should be developed (Rusinova, 2015, p. 207).

The assessment of whether IT specialists "directly participate in hostilities" may be conducted on the grounds of compliance with minimal gravity threshold of harm, the link between the act and ongoing military actions and the causal link between the act and the harm. The neutrality of these criteria implies the possibility of their application to the malicious use of ICTs by IT specialists during an armed conflict (Schmitt, 2017, Rule 97). The timeframe for "direct participation" is also indicative.

---

68 GC I, GC II, GC III, Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (12 August 1949), 75 UNTS 287, Common Article 3(1).

69 AP I. Articles 51(3), 67(1)(e).

70 AP II. Article 13(3).

71 *Prosecutor v. Dusko Tadic a/k/a "DULE"* [7 May 1997] ICTY Trial Chamber II, Judgement, para. 616.

72 See, for example, IACommHR, *Third Report on the Human Rights Situation in Colombia*, Chapter IV, para. 51.

"Hostilities" are defined as acts that "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" (Melzer, 2009, p. 47). This definition should also include a criterion according to which the damage inflicted by the act must reach minimal gravity threshold. Moreover, this gravity should relate to both attacks on civilians and civilian objects as well as military objectives. In case of military objectives, the threshold may be deduced from the IHL norms' main content regulating damaging the adversary by killing, wounding and destroying or damaging property (Rusinova, 2015, pp. 210–211). To qualify acts of civilians as DPH, they must have inflicted, or be objectively likely to inflict damage on one of the parties and be committed in connection with an ongoing armed conflict. Thus, the link between the act and military actions must also be demonstrated (Melzer, 2009, pp. 46–64). However, it should not matter whether the person committing such actions represents another party to the conflict or not.[73]

Since malicious use of ICTs rarely leads to violent physical consequences, it is sometimes pointed out that 'digital' harm is manifested when malicious use of ICTs has a negative impact on the adversary's military capabilities or activity (Schmitt, 2017, Rule 97). Examples of DPH using digital means may involve causing damage to the opponent's possessions or equipment, or conveying military information for the belligerent's instant exploitation.[74] If the damage caused by the actions of IT specialists is not aimed at military objectives, "it must be very likely to cause death, injury or destruction on protected persons or objects".[75] Sometimes it is also stated that the harm from malicious use of ICTs terrorizing civilian population in the sense of "inhuman treatment", i. e. "severe physical or mental suffering", may also attain the threshold.[76] In any event, expanding of the minimal gravity threshold must be done in a very cautious manner as it would extend the DPH category raising the range of potential IT specialists who could be subject to attacks (Biggio, 2024, p. 167).

Analysing the causal link between the acts and the damage inflicted, the ICRC recommends to qualify acts as DPH if the damage is brought about "in one causal step". At the same time direct preparatory acts are also covered. Such controversial examples as the delivery of combatants, weapons, ammunition, and military equipment to and from the battlefield by a civilian driver (opposing to general logistical functions) as "an integral part of ongoing combat operations" (Melzer, 2009, pp. 53–54, 56) as well as planning and strategic

---

73 *Prosecutor v. Jean-Paul Akayesu* [2 September 1998] ICTR Trial Chamber Judgment, para. 444.

74 Direct participation in hostilities. In Mačák, K., Minárik, T., Jančárková, T. (Eds). *Cyber Law Toolkit (2019-)*. URL: https://cyberlaw.ccdcoe.org/wiki/Direct_participation_in_hostilities#cite_note-5.

75 Kostadinov, D. *Jus in Cyber Bello*.

76 Ibid.

direction of military operations must also constitute DPH[77] (Rusinova, 2015, pp. 214–216).

This requirement may be problematic in the cyber realm as malicious use of ICTs often leads to "second order"[78] or reverberating consequences. "First order" consequences are immediate and direct while "second order" ones are delayed and generated through intermediate events. For instance, the loss of a system's functionality reflects the "first order" effect while the ramifications flowing from such a functionality loss for an adversary's military capacity demonstrate "second order" effects (Biggio, 2024, pp. 167–168). Excluding such effects would also exclude many types of malicious use of ICTs from attaining this threshold (Turns, 2012, p. 288). Thus, a balanced approach may be to accept reverberating consequences that are linked to the initial malicious use of ICTs by "an uninterrupted causal chain" (Biggio, 2024, p. 168). Meanwhile, "*causal* proximity… should not be confused with… *temporal* or *geographic* proximity" (Melzer, 2009, p. 55). Anonymity and secrecy of many cyber acts may also complicate the assessment (Biggio, 2024, p. 168).

Another important aspect is the timeframe for DPH. On the one hand, sometimes periods of civilians' DPH and losing protection from attack are distinguished to avoid the "revolving door" phenomenon which supposedly gives an unreasonably extended immunity from attack.[79] However, members of terrorist and other armed groups who have a DPH function move from the category of civilians to combatants (Rusinova, 2015, p. 217–218). If such a group does not meet the criteria of an organised armed group, this person must perform a continuous combat function such as preparing, conducting or leading acts attaining the needed minimal gravity threshold to be able to be qualified as DPH (Melzer, 2009, p. 34). This is crucial for eliminating auxiliary support functions from the DPH category. Thus, the periods of DPH and losing protection from attack must coincide to avoid the qualification based on assumptions and presumptions rather than specific actions (Crawford, 2013, p. 12). At the same time, the ICRC clarifies that preparations for a particular operation, the phase of deployment and return after it should also be considered as DPH (Pilloud, Sandoz, Swinarski, & Zimmermann, 1987, para. 1943).

---

77 *Prosecutor v. Pavle Strugar* [17 July 2008] ICTY Appeals Chamber Judgement, paras. 164, 180–185; *USA v. Salim Ahmed Hamdan* [19 December 2007], United States Court of Military Commission, p. 6; *The Public Committee Against Torture et al. v. The Government of Israel et al.* [13 December 2006] Israel High Court of Justice Judgment, para. 35.

78 Joint Chiefs of Staff, Armed Forces of the United States (31 January 2013). *Joint Targeting*, pp. 11–35.

79 In such a case each terrorist has "horns of the alter"… to grasp or a "city of refuge"… to flee to, to which he turns in order to rest and prepare while they grant him immunity from attack." Israel HCJ, *The Public Committee Against Torture*, para. 40.

Since the performance of IT specialists acts does not require geographic relocation, the time limits of DPH involve only the moment of the acts' execution and preparatory steps constituting an essential part of the malicious use of ICTs.[80] Thus, the period of targetability is "practically non-existent" (Biggio, 2024, p. 169; Wallace, Reeves, & Powell, 2021, p. 186; Melzer, 2009, p. 53) as even preparatory phase may often be evaluated only afterwards. At the same time the acts' planning and the actions before the active role in them terminates may also be counted. Thus, it may not be identical to the period when the harm takes place (Schmitt, 2013, Rule 35(8)) while still difficult to evaluate. Another problematic issue arises from multiple acts of malicious use of ICTs over a particular period. The majority of Tallinn Manual drafting experts consider such acts as isolated, while the minority regard the whole such period as targetability 'window' (Schmitt, 2017, p. 432; Melzer¸ 2009, pp. 44–45, 70–71) until the actor "unambiguously opt[s] out of hostilities through extended non-participation or an affirmative act of withdrawal" (Schmitt, 2004, pp. 511, 534; Watkin, 2005, pp. 137–167). Nevertheless, the practical possibility of such targeting is also questionable.

If an IT specialist is simply a member of a hacktivist group which does not meet the criteria of an organized armed group, it will not amount to continuous combat function (Melzer, 2009, pp. 33–35). According to the classification of D. Turns, among such categories of IT specialists as "those who design and write the programs used" for malicious use of ICTs, "those who install these programs on the computer systems, act as service administrators and provide technical maintenance for them" and "those who actually operate the computer programs" during malicious acts of ICTs use, the members of the last category are more likely to reach DPH threshold. However, the issue of "civilian scientists and weapons experts" is rather vague as they tend to be considered as indirectly participating and, thus, protected as civilians. Besides, although "armed attack" does not cover "espionage and exploitation operations" (Turns, 2012, pp. 289, 295), hostilities are broad enough in their scope to encompass them.

Addressing national positions, France refers to such potential examples of DPH as "the penetration of a military system by a party to an armed conflict with a view to gathering tactical intelligence for the benefit of an adversary for the purposes of an attack… installing malicious code, preparing a botnet in order to launch an attack by denial of service, or developing software specifically

[80] Prescott, J. M. (2012). Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States?. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (pp. 1–16). IEEE.

intended for the perpetration of a hostile act".[81] Thus, "civilians conducting offensive activities" amounting to DPH may "be targeted by conventional means".[82] Germany provides examples of "electronic interference with military computer networks… whether through computer network attacks or computer network exploitation, as well as wiretapping [of an] adversary's high command or transmitting tactical targeting information for an attack".[83] The US even regards the status of persons "belonging to a non-state armed group as a separate basis upon which a person is liable of attack, apart from whether he or she has taken a direct part in hostilities" (Preston, Taylor, 2016, p. 236). These approaches may be considered overly broad as the needed thresholds are sometimes neglected making civilians a target of attack.

As a practical example, a pager attack against Hezbollah members allegedly carried out by Israel[84] in September 2024 caused more than several dozen deaths and 4000 injuries. This act was called a "cyber operation" and, proving NIAC existence, it may be qualified as a cyber "attack." The identity of its participants is not known but if they are not organised armed groups' or armed forces' members, the gravity threshold might allow their actions to be qualified as DPH.

Concluding with the rights and protection of IT specialists qualified as "directly participating in hostilities", they enjoy the protection afforded to civilians both in IAC and NIAC correspondingly unless and for such a period they "directly participate in hostilities" (Henckaerts et al., 2006, Rule 6). They are not afforded a POW status with corresponding protection and combatant immunity. Thus, although the application of this category may be also problematic given the specificity of the cyber sphere, it seems to be one of rather balanced approaches provided the periods of DPH and losing protection from attack coincide and all the thresholds are met.

Conclusion

Current research has demonstrated the difficulties of the existing IHL regulation application to adequately assess IT specialists' status in real armed conflicts. On the one hand, the IHL rules were formulated in such a way that allows them to

---

81 Ministry of Defense of France (9 September 2019). *International Law Applied to Operations in Cyberspace*, p. 15.

82 Ibid.

83 Federal Government of Germany (2021) *Position Paper On the Application of International Law in Cyberspace*, p. 8.

84 Hezbollah pager attack puts spotlight on Israel's cyber warfare Unit 8200 (20 September 2024). *Reuters*. URL: https://www.reuters.com/world/middle-east/hezbollah-pager-attack-puts-spotlight-israels-cyber-warfare-unit-8200-2024-09-18/.

apply to the widest possible number of weapons including future ones.[85] On the other hand, many questions posed by the developing technological world, which could not have been foreseen in advance, raise heated debates. This is particularly relevant to the cyber sphere. The lack of a clear distinction between the military use of ICTs, which can be qualified under *jus in bello* and non-military use encompassed by international human rights law and national criminal law, may result in the abuse of the military paradigm. In other words, invoking IHL as a *lex specialis* may be used by States to avoid the application of more suitable regimes and to shield their activities (Rusinova & Martynova, 2023, p. 150).

IHL terminological limits compromise the possibility of assigning IT specialists to a particular category of persons within an armed conflict. This mix of possible statuses creates a risk for other civilians who may be confused with IT specialists, especially given that they often operate from urban areas far from the battlefield. In some cases, the present rules demonstrate their definite practical inapplicability to real cases in the cyber realm. IHL norms do not consider such new capacities as remote location of IT specialists so that the theatre of war is the whole world. Thus, such statuses as POW become losing their relevance.

The difficulty of relating IT specialists to lawful combatants meeting the required criteria may also result in a paradoxical situation where combatants using traditional lethal force and weapons which may cause civilian harm with higher probability are often better protected than potential 'cyber' combatants (e. g. POW guarantees etc.) (D'Urso, 2015, p. 2). On the contrary, IT specialists located miles away from the battlefield may have much greater influence and capabilities than traditional soldiers. Therefore, such new actors' status and consequent rights and protection should be properly and clearly defined according to the law of armed conflict too.

The analysis showed that the qualification of an IT specialist as a part of regular armed forces during IAC seems to be less controversial than as a part of irregular ones in IAC or organised armed group in NIAC. *Levée en masse* category may be suitable considering the spontaneous and unorganised nature of many IT specialists' activities but it has significant limitations not adjusted to new cyber actors. Some IT specialists perform only civilian functions and may be qualified only as such.

The DPH qualification sometimes may be the best perspective due to the civilization of modern armed conflicts, however, it has its own ambiguities. The main risk is the potentially growing violence amount which can be legitimately

[85] ICJ. *Nuclear Weapons*, para. 86.

used against such participants and subsequent collateral damage (Rodenhäuser & Vignati, 2023) among the whole civilian population. This threat might be balanced by the application of relevant IHL principles of precautions, proportionality and at the same time military necessity. Besides, the verification of direct participants may be very complicated in practice. Nevertheless, civilians who directly participate in hostilities on a permanent basis are at a higher risk of being attacked.

Thus, the operation relating to disrupting Iran's uranium enrichment centrifuges through Stuxnet malware was reportedly performed at the urging of the USA and Israel governments (Schmitt, 2015, p. 1112). An armed conflict was not in existence, thus, IHL is not applicable. If it was and if this malicious use of ICTs was not conducted by armed forces units, it potentially may be an illustrative example of reaching the DPH threshold according to the gravity of physical damage caused. In any event, the virus had to initially spread among many civilian computers to reach its final goal. This example demonstrating the presence of cyber perfidy[86] may show the negative influence on non-military targets and the situation of impunity of such offenders. DDOS attacks usually performed by a network of hacktivists upon suspicion of State involvement also contribute to the attribution problem. In the cyber realm States often refer to proxies and non-State intermediaries. However, the establishment of responsible persons is a very complex issue, especially according to existing tests. In general, given the complexity of the attacker identification, the retaliatory targeting “remains marginal”.[87]

Overall, the fact that most contemporary cyber acts do not trigger physical consequences and do not attain a minimal gravity threshold cannot be neglected. Other elements of analysed categories are also problematic due to specifics of the cyber realm. Thus, a very limited number of IT specialists should be qualified other than as civilians and only if the necessary requirements are met. *De lege ferenda*, adjusting the interpretation of DPH category as the most suitable to IT specialists might be a possible solution. For instance, new ICRC commentary[88] has provisions on “cyber operations”. However, such adjustments should be done cautiously to avoid overly broad interpretation and excessive militarisation.

[86] Kostadinov, D. *Jus in Cyber Bello.*

[87] Ministry of Defense of France (9 September 2019). *International Law Applied to Operations in Cyberspace*, p. 15.

[88] ICRC. Commentary on GC I.

Список литературы / References

1. Русинова, В. Н. (2015) *Права человека в вооруженных конфликтах: проблемы соотношения норм международного гуманитарного права и международного права прав человека*. Статут.
   Rusinova, V. N. (2015). *Human rights in armed conflicts: problems of correlation of international humanitarian law and international human rights law*. Statut.
2. Biggio, G. (2024). The legal status and targeting of hacker groups in the Russia-Ukraine cyber conflict. *Journal of International Humanitarian Legal Studies*, *15*(1), 142–182. https://doi.org/10.1163/18781527-bja10078
3. Buchan, R. & Tsagourias, N. (2022). Ukranian 'IT Army': a cyber *levée en masse* or civilians directly participating in hostilities? *EJIL:Talk!*. Available at:https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/
4. Buchan, R. (2016). Cyber warfare and the status of anonymous under international humanitarian law. *Chinese Journal of International Law*, *15*(4), 741–772. https://doi.org/10.1093/chinesejil/jmw041
5. Cassese, A. (2007). On some merits of the Israeli judgement on targeted Killings. *Journal of International Criminal Justice, 5*(2), 339–345. https://doi.org/10.1093/jicj/mqm012
6. Crawford, E. (2013). Virtual backgrounds: direct participation in cyber warfare. *Sydney Law School Research Paper*, 10/12. Available at: https://ssrn.com/abstract=2001794.
7. D'Urso, M. (2015). The cyber combatant: a new status for a new warrior. *Philosophy & Technology*, *28*(3), 475–478. https://doi.org/10.1007/s13347-015-0196-9
8. Dinstein, Y. (2013). Cyber war and international law: concluding remarks at the 2012 Naval war college international law conference. *International Law Studies*, *89*(1), 159–169. https://doi.org/10.1163/9789004242081_008
9. Dinstein, Y. (2022). *The conduct of hostilities under the law of international armed conflict*. Cambridge University Press. https://doi.org/10.1017/9781009106191
10. Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246
11. Geiß, R. & Lahmann, H. (2012). Cyber warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, *45*(3), 381–399. https://doi.org/10.1017/s0021223712000179

12. Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: international humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, *102*(913), 287–334. https://doi.org/10.1017/s1816383120000387
13. Henckaerts, J.-M., Doswald-Beck, L., Alvermann, C., Dörmann, K., & Rolle, B. (2005). *Customary international humanitarian law*. Cambridge University Press. https://doi.org/10.1017/cbo9780511804700
14. ICRC. (2021). *Commentary on the Third Geneva Convention*. Cambridge University Press. https://doi.org/10.1017/9781108979320
15. ICRC. (2020). International humanitarian law and cyber operations during armed conflicts: ICRC position paper. *International Review of the Red Cross, 102*(913), 481–491.
16. Mačak, K. & Schmitt, M. N. (2018). Enemy-controlled battlespace: the contemporary meaning and purpose of Additional Protocol I's Article 44 (3) Exception. *Vanderbilt Journal of Transnational Law, 51*(5), 1353–1380.
17. Melzer, N. (2009). *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. ICRC.
18. Melzer, N. (2011). *Cyberwarfare and international law*. UNIDIR.
19. Pfanner, T. (2004). Military uniforms and the law of war. *International Review of the Red Cross*, *86*(853), 93–130. https://doi.org/10.1017/s1560775500180113
20. Pictet, J. S. (1960). *Commentary on the Geneva Conventions of 12 August 1949.* ICRC.
21. Pilloud, C., Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.). (1987). *Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Martinus Nijhoff Publishers.
22. Preston, S. E., & Taylor, R. S. (2016). *Department of defense law of war manual*. General Counsel of the Department of Defense Washington United States. https://doi.org/10.1017/9781108659727.
23. Rodenhäuser, T. & Vignati, M. (4 October 2023). 8 rules for “civilian hackers” during war, and 4 obligations for states to restrain them. *EJIL:Talk!*. Available at: https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/
24. Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001
25. Rusinova, V. N. (2022). Qualification of harmful use of information and communications technologies under international law: in search of a

consensus. *Moscow Journal of International Law*, 1, 38–51 https://doi.org/10.24833/0869-0049-2022-1-38-51
26. Rusinova, V. & Martynova, E. (2023). Fighting cyber attacks with sanctions: digital threats, economic responses. *Israel Law Review*, *57*(1), 135–174. https://doi.org/10.1017/s0021223722000255
27. Sassoli, M. & Bouvier, A. (2008). *Legal protection in time of war*. ICRC.
28. Schmitt, M. N. (2004). Humanitarian law and direct participation in hostilities by private contractors or civilian employees. *Chicago Journal of International Law*, *5*(2), 511–546.
29. Schmitt, M. N. (2011). Cyber operations and the *jus in bello*: key issues. In *Israel Yearbook on Human Rights*. Vol. 41 (pp. 113–135). Brill Nijhoff. https://doi.org/10.1163/9789004226449_006
30. Schmitt, M. N. (2012). Classification in future conflict. In E. Wilmshurst (Ed)., *International law and the classification of conflicts* (pp. 455–477). Oxford Academic. https://doi.org/10.1093/law/9780199657759.003.0014
31. Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/cbo9781139169288
32. Schmitt, M. N. (2015). The use of cyber force and international law. In M. Weller (Ed.), *The Oxford handbook of the use of force in international law*. Oxford Academic. https://doi.org/10.1093/law/9780199673049.003.0053
33. Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524
34. Turns, D. (2012). Cyber warfare and the notion of direct participation in hostilities. *Journal of conflict and security law*, *17*(2), 279–297. https://doi.org/10.1093/jcsl/krs021
35. Wallace, D. A. & Reeves, S. (2013). The law of armed conflict's' wicked' problem: *levée en masse* in cyber warfare. *International Law Studies, 89*, 646–668.
36. Wallace, D., Reeves, S., & Powell, T. (2021). Direct participation in hostilities in the age of cyber: exploring the fault lines. *Harvard National Security Journal*, 12, 164–197.
37. Waters, C. (2014). New hacktivists and the old concept of *levée en masse*. The *Dalhousie Law Journal*, *37*(2), 772–786.
38. Watkin, K. (2005). Humans in the cross-hairs: targeting and assassination in contemporary armed conflict. In D. Wippman & M. Evangelista (Eds.), *New wars, new laws? Applying laws of war in 21st century conflicts* (pp. 137–179). Brill Nijhoff. https://doi.org/10.1163/9789004479692_008