ACTA UNIVERSITATIS LODZIENSIS
FOLIA IURIDICA 106, 2024

https://doi.org/10.18778/0208-6069.106.06

COPE Member since 2018 JM13714

*Michał Byczyński**

https://orcid.org/0000-0001-6856-0627

THE LEGAL STATUS OF 'CIVILIAN HACKERS' UNDER INTERNATIONAL HUMANITARIAN LAW

Abstract. In response to the rising trend of civilian hackers participating in cyber conflicts, the International Committee of the Red Cross has recently issued guidelines regulating their conduct. This article navigates the intricate legal landscape surrounding civilians who actively participate in cyber hostilities, exploring the concept of direct participation in hostilities (DPH) in the context of cyber warfare. Given the unique nature of cyber warfare, the article highlights the need for a nuanced and context-specific approach in determining the legal status of civilians involved in cyber hostilities. It underscores the importance of distinguishing between actions linked to an ongoing armed conflict and those that occur independently. The piece discusses the challenges in defining civilians in cyber warfare, the principles of distinction and proportionality, the criteria for qualifying a civilian as a "direct participant of hostilities" and the concept of continuous combat function (CCF), which distinguishes civilians continuously involved in cyber hostilities from those sporadically or *ad hoc* engaged. The article also delves into the temporal challenges in cyber operations and the "revolving door" concept, which complicates the application of DPH status in cyber warfare.

Keywords: cyberwar, hacktivists, civilian hackers, direct participation in hostilities, Russia-Ukraine war

STATUS PRAWNY CYWILNYCH HAKERÓW W ŚWIETLE MIĘDZYNARODOWEGO PRAWA HUMANITARNEGO

Streszczenie. W odpowiedzi na rosnącą liczbę cywilnych hakerów uczestniczących w różnego rodzaju aktywnościach cybernetycznych, Międzynarodowy Komitet Czerwonego Krzyża opublikował wytyczne dotyczące podejmowanych przez nich tego rodzaju działań. W niniejszym artykule omówiono regulacje prawne dotyczące cywili, którzy biorą udział w działaniach zbrojnych w cyberprzestrzeni, opierając analizę przede wszystkim na koncepcji bezpośredniego uczestnictwa w działaniach zbrojnych w kontekście wojny cybernetycznej. Ze względu na szczególny charakter wojny cybernetycznej, podkreślono potrzebę zastosowania kontekstowego i indywidualnego podejścia celem określenia statusu prawnego cywili zaangażowanych w działania zbrojne w cyberprzestrzeni. W artykule omówiono trudności w definiowaniu cywili w wojnie cybernetycznej, zasady rozróżnienia i proporcjonalności, kryteria kwalifikacji cywila jako „bezpośredniego uczestnika działań zbrojnych" oraz koncepcję ciągłej funkcji bojowej, która odróżnia cywilów stale zaangażowanych

* University of Lodz, Doctoral School of Social Sciences, mbyczynski@lodz.adwokatura.pl

Received: 5.11.2023. Verified: 8.11.2023. Revised: 8.11.2023. Accepted: 17.11.2023.

w działania zbrojne w cyberprzestrzeni od tych działających okresowo czy *ad hoc*. Poruszono również problemy związane z aspektami czasowymi operacji w cyberprzestrzeni i koncepcję „revolving door", która utrudnia precyzyjne określenie statusu prawnego cywilnych hakerów w kontekście wojny cybernetycznej.

Słowa kluczowe: cyberwojna, haktywiści, cywilni hakerzy, bezpośrednie uczestnictwo w działaniach zbrojnych, wojna rosyjsko-ukraińska

1. INTRODUCTION

The International Committee of the Red Cross [ICRC] has recently published a set of rules aimed at regulating the conduct of civilian hackers involved in conflict situations (ICRC 2023). This development comes in response to a growing trend of people joining patriotic cyber groups following the Ukraine invasion. These guidelines, consisting of eight key rules, include provisions that prohibit attacks on hospitals, the creation of hacking tools that can spread uncontrollably, and the making of threats that terrorise civilian populations.

In a rapidly changing world where warfare transcends traditional boundaries, cyber conflict has emerged as a powerful and unconventional battleground. This new form of warfare challenges established legal frameworks, raising questions about the status of those who engage in hostilities through cyber means. Ukraine's ongoing conflict with Russia has provided a real-world backdrop to these inquiries, as civilian hackers, driven by the desire to support Ukraine, target Russian entities.[1]

As we navigate this evolving landscape, it becomes essential to understand the legal status of civilians who actively participate in hostilities through cyber operations (civilian hackers). International humanitarian law (IHL) traditionally distinguishes between combatants and civilians in armed conflicts under the principle of distinction. However, the rise of cyber warfare blurs these lines, making the legal status of engaged civilians more complex.

This article delves into the realm of civilian direct participation in cyber hostilities, especially as it relates to the conflict in Ukraine. The aim is to explore the notion of direct participation in hostilities (DPH), keeping in mind the actions of cyberactivisits responding to the ongoing conflict. Moreover, the article addresses unique aspects of cyber warfare, such as civilians operating beyond the geographical limits of the armed conflict and their anonymity on the Internet.

By exploring these complex issues, the article seeks to shed light on the intricate legal status of civilian hackers operating within the context of the Ukrainian conflict. This article is inspired by the actions of hacktivists in response to the ongoing war in Ukraine, aiming to provide insights into their legal standing and the evolving nature of warfare in the digital age. The analysis will be conducted in several interconnected chapters, each contributing to a thorough understanding of this evolving landscape.

[1] See: Tidy (2022; 2023).

2. CIVILIANS IN THE CROSSFIRE – DECIPHERING PROTECTION UNDER IHL

International humanitarian law, a specialised segment of international legal norms, serves as a framework that regulates and confines conduct during times of armed conflict. These principles and standards find expression in legal instruments such as the 1949 Geneva Conventions and their 1977 Additional Protocols, as well as customary international law. The primary aim of IHL is to mitigate the detrimental consequences of warfare, especially regarding civilians, that is non-participating individuals (Melzer 2016, 17).

Defining whether an individual qualifies as a civilian, based on their status rather than their actions, is a complex and distinct issue. Art. 50 of Protocol Additional to the Geneva Conventions of 12th August, 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8th June, 1977, 1125 UNTS 3, offers a definition of a civilian as "any person who does not belong to one of the categories of the persons referred to in Art. 4A (1), (2), (3), and (6)"[2] and when in doubt, a person should be presumed a civilian. While this definition aids in identifying civilians, it does not offer guidance on the legal perception of civilians who engage in hostilities.

The principle of distinction, which mandates that attacks must clearly differentiate between civilians and combatants, as well as between civilian and military targets, plays a pivotal role in international humanitarian law. It serves as the foundation for regulating the conduct of parties involved in armed conflicts and is enshrined in Arts. 51–52 Protocol I.

This principle not only prohibits direct attacks on civilians or civilian objects but goes further to explicitly forbid any acts of violence primarily intended to terrorise the civilian population, as stipulated in Art. 51(2)

[2] Article 4(A) (1), (2), (3) and (6) of the Third Geneva Convention (Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12th August, 1949):

(1) Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.

(2) Members of other militias and members of other volunteer corps, including those of organised resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organised resistance movements, fulfil the following conditions:

(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognisable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war.

(3) Members of regular armed forces who profess allegiance to a government or an authority not recognised by the Detaining Power.

(6) Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.

Protocol I. Furthermore, it expressly bans any attacks that do not adequately distinguish between civilians and combatants, as outlined in Art. 51(4) Protocol I.

Additionally, the principle of proportionality, stated in Art. 51(1)(b) Protocol I, establishes that every attack leading to collateral damage, which results in civilian casualties, injuries, or damage to civilian property, must be proportionate to the specific and direct military advantage anticipated from the attack. These comprehensive protections for civilians are frequently referred to as "non-combatant immunity", emphasising the fundamental safeguard provided by IHL to individuals who do not take part in hostilities (Lazar 2013, 1).

As mentioned, Art. 51(2) Protocol I explicitly prohibits any attacks on the civilian population and individual civilians. This provision generally means that civilian hackers typically steer clear of involvement in armed conflicts as per international humanitarian law. However, Art. 51(3) Protocol I adds the condition that civilians enjoy protection "unless and for such time as they take a direct part in hostilities."[3] This prompts a significant consideration whether the actions of civilian activists qualify as 'direct participation' in the ongoing Russia-Ukraine war. Safeguarding civilians and adhering to the principle of distinction are fundamental aspects of international humanitarian law reflecting customary international law (Supreme Court of Israel, Public Committee against Torture in Israel v. Government of Israel, Case No. HCJ 769/02, 13th December, 2006, 46).

It is thus paramount to recognise the importance of distinguishing civilians from combatants in the context of these legal principles, as the consequences bear directly on the level of protection they receive during armed conflicts. Clarity in identifying who qualifies as a civilian and who does not is vital for upholding the integrity of international humanitarian law and ensuring that civilians are shielded from the horrors of warfare to the greatest extent possible.

Concluding the analysis of the foundational principles that govern the protection of civilians under international humanitarian law, the transition to the intricate realm of direct participation in (cyber)hostilities becomes imminent. The forthcoming exploration delves into the actions of civilian activists, probing the nuanced boundaries of their engagement within the established legal framework. This shift in focus leads to a comprehensive examination of the dynamic discussions surrounding direct participation in (cyber)hostilities, as well as the evolving interpretations provided by legal scholars and institutions in response to the challenges posed by modern conflict scenarios.

[3] The very same approach is visible in Art. 13(3) Protocol II focusing on the protection of victims in non-international armed conflicts. Civilians are offered a protection conditionally, meaning that they are protected unless and for such time as they take a direct part in hostilities. By acknowledging the conditional nature of protection, this legal provision acknowledges the dynamic and fluid nature of conflict situations, where the status of individuals may change based on their actions and involvement in hostilities.

3. DIRECT PARTICIPATION IN (CYBER)HOSTILITIES

It can be assumed that the cyberattacks by activists against the Russian government are a reaction to the war, clearly intended to support the Ukrainian side. This central issue revolves around whether these actions attain the necessary level of significance within international humanitarian law. The assessment of whether a civilian is actively participating in the ongoing conflict is not contingent on their status or affiliations but on their involvement in specific hostile activities (Schmitt 2017, 413). The mode of operation for activists, be it random, impulsive, or disorganised, is not of primary importance.

The regulations concerning the targeting of civilians remain unchanged, whether in an international (as in the Russo-Ukrainian case) or non-international armed conflict (Buchan 2016, 21). Nevertheless, in the context of both types of conflicts, civilians can become subject to direct targeting when they engage in direct participation in hostilities (Buchan 2016, 21–22).

However, there is no defined guidance provided in treaty law for the definition of 'direct participation in hostilities', although this concept seems crucial when determining legal status of civilians engaged in conflict-related behaviours.

In response to the uncertainty surrounding the concept of direct participation in hostilities, the International Committee of the Red Cross undertook research and engaged in expert consultations to elucidate the conditions under which a civilian may be considered as directly involved in hostilities. It is essential to emphasise that the ICRC's work, while addressing this issue, does not seek to modify the existing legal framework but, rather, offers an interpretation of the concept of direct participation in hostilities within the established boundaries (Melzer 2009, 6).

In May 2009, the ICRC issued the Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law (Guidance). The Guidance faced substantial criticism, with numerous voices contending that it embraced an excessively restrictive interpretation of the concept of direct participation in hostilities (Schmitt 2010a, 720[4]). Nevertheless, for the purpose of determining the legal status of civilians involved in hostilities, this article presumes the legal significance of the Guidance because of its growing respect and worldwide recognition (Longobardo 2017, 828[5]).

[4] See also: Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions (2010, 66–67).

[5] See also: Akande (2010, 180 et seq).

4. CRITERIA TO QUALIFY A CIVILIAN AS A DIRECT PARTICIPANT IN HOSTILITIES

As per the ICRC's Guidance, for cyber operations to be considered legally relevant actions under international humanitarian law, they need to meet three specific criteria. First, these operations must reach a specific threshold of harm (4.1). Second, they must directly result in that harm (4.2). And third, they must be designed with the intent of supporting one party in the conflict over the other, a requirement known as the belligerent nexus (4.3). In addition, the notion of continuous combat function is a pivotal supplement to the three criteria set by the DPH framework (4.4).

4.1. How severe should the harm be?

The first threshold, referred to as the 'threshold of harm', requires that "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" (Melzer 2009, 46–50). This indicates that even if the desired result has not happened yet, the act's repercussions must be likely to lead to it. As a result, the probability of harm is adequate to meet the harm threshold. This suggests that there is an objective probability that harm that can be objectively identified will be caused whenever a citizen has a subjective desire to do so (Schmitt 2010a, 725). On the other hand, the threshold of harm can also be reached by doing "harm of a specifically military nature or by inflicting death, injury, or destruction on persons or objects protected against direct attack" (Melzer 2009, 47).

According to the Guidance, "the interruption of electricity, water, or food supplies, (…) the manipulation of computer networks, (…) would not, in the absence of adverse military effects, cause the kind and degree of harm required to qualify as direct participation in hostilities" (Melzer 2009, 50).

This becomes particularly relevant when we delve into the realm of cyberwarfare. Although relatively uncommon, cyberattacks can undeniably lead to fatalities, severe injuries, or significant destruction. Consequently, it becomes evident that a cyber operation encounters challenges in meeting the civilian aspect of the threshold of harm.

The primary focus of the Guidance is on harm occurring in the physical world (Prescott 2012, 253). In the realm of cyberspace, the absence of immediate loss of life or physical injuries might be conspicuous, but it is clear that the vulnerability of data to loss or damage is ever-present. The concept of damage or destruction to data could arguably surpass the threshold of harm, particularly in critical contexts such as government or military databases, where the implications can be substantial.

When it comes to the military aspect of the harm threshold, which necessitates that it must "adversely affect military operations or military capacity," (Melzer 2009, 50) cyber operations seem to offer a more attainable avenue. Cyberattacks have the potential to be highly disruptive and can significantly impact military capacity. Nonetheless, there is ongoing debate as to whether a specific cyberattack genuinely affects military capacity or merely serves as a form of expression, propaganda, or a minor nuisance (Kilovaty 2016, 12). Additionally, the Guidance acknowledged the possibility of cyberattacks affecting military capacity by suggesting that "electronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitations (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack" (Melzer 2009, 48).

4.2. One step back

The second criterion, the so-called 'direct causation' condition, requires that "there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part" (Melzer 2009, 46, 51–57).

In simpler terms, a particular activity must be capable of independently causing the harm. Alternatively, it can also fulfil the direct causation requirement if it is an essential and integral component of a combined military operation that is reasonably expected to lead to the required level of harm (Schmitt 2010a, 727–728). In essence, this criterion underscores the need for a direct, cause-and-effect relationship between the action in question and the harm that is either directly produced or reasonably anticipated.

The predominant method for determining causation involves evaluating whether the harm can be traced back to the act with just a single causal step in between (Kilovaty 2016, 12). When it comes to cyber operations, they do not significantly pose a challenge to this criterion. The action's causal relationship to the expected or actual injury remains intact, even if it takes place outside the battlefield in its traditional – physical – meaning (Melzer 2009, 55).

The cascading nature of effects in the realm of cyber operations can be likened to a chain reaction, where each step in the process contributes to the eventual outcome. These multi-step causal chains can involve a series of interconnected systems, often including unwitting intermediaries who play a role in transmitting the impact. This intricate web of cause and effect can make it considerably more challenging to directly attribute the harm to the initial cyber operation, particularly when it involves a complex network of compromised systems.

Furthermore, the rapidly evolving landscape of cyber threats and vulnerabilities adds another layer of complexity to assessing direct causation

in cyber operations. As technology and tactics evolve, the interconnectedness of systems and the potential for harm to ripple through various layers of infrastructure only intensify. This dynamic environment underscores the need for a nuanced approach to understanding the causal links in cyber conflicts (Turns 2012, 288 et seq.).

4.3. Belligerent nexus

The 'belligerent nexus' requirement plays a vital role in distinguishing actions that are tied to the dynamics of an armed conflict from those that occur independently. Its significance lies in two primary functions.

First, the requirement is a targeted tool aimed at capturing actions that take place within the specific context of an armed conflict. It focuses on those actions that are strategically designed to tip the scales in favour of one party involved in the conflict while causing harm to the opposing side. In essence, it seeks to identify and hold accountable individuals whose actions are strategically aligned with the objectives of one of the conflicting parties (Melzer 2009, 58).

Secondly, the belligerent nexus requirement serves as a filter that screens out actions that, though they may result in the requisite level of harm, occur independently of any ongoing armed conflict. In such cases, where the harm is directly caused by the act but the act itself lacks a strategic connection to the conflict, the civilian involved is not classified as a DPH. Consequently, these individuals are subject to standard legal processes and law enforcement procedures, as their actions do not meet the criteria set forth by the belligerent nexus requirement. This nuanced criterion ensures that individuals are held accountable within the appropriate legal framework based on the nature of their actions in relation to the conflict (Melzer 2009, 64).

5. CONTINUOUS COMBAT FUNCTION – THE DIFFERENCES BETWEEN CCF CIVILIAN AND DPH CIVILIAN

The concept of 'continuous combat function' [CCF] stands as a significant complement to the principles associated with the framework of direct participation in hostilities (Melzer 2009, 33). The conventional understanding of the DPH status holds that it is time-bound, applying solely to civilians during the period when they actively engage in hostile actions (Art. 51(3) Protocol I). This implies that individuals who sporadically, spontaneously, or in an uncoordinated manner carry out such actions are susceptible to being targeted exclusively during the execution of those actions.

However, the introduction of the CCF principle introduces an important distinction. When a civilian assumes an integral role within an organised armed

group and his/her tasks are related to the preparation, execution, or command of acts amounting to direct participation in hostilities, he/she acquires the CCF status. Under the CCF principle, such a civilian can be targeted even when he/she is not actively involved in hostile actions at the precise moment of targeting (Melzer 2009, 34). Essentially, the CCF civilian becomes a potential target based on their status, which solidified due to their persistent and consistent involvement.

On the other hand, a DPH civilian is only subject to targeting during the specific instances when he/she is actively engaged in hostile actions. This implies that a civilian forfeits his/her protection against direct attacks only for the duration of each distinct act constituting direct participation in hostilities.

Members of organised armed groups involved in an armed conflict cease to be civilians and relinquish their protection against direct attacks for as long as they maintain their CCF (Melzer 2009, 70). A hacker who continuously conducts cyber-attacks within an armed conflict and is a member of an organised armed group participating in the conflict would be holding a CCF. Consequently, such a person can be considered a potential target at all times, as long as he/she retains the CCF status.

6. PREPARATORY MEASURES, DEPLOYMENT, AND RETURN – WHEN DOES THE DPH START?

In accordance with section VI of the Guidance it is stated that "measures preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution, constitute an integral part of that act" (Melzer 2009, 66). In other words, the determination of whether preparatory measures constitute direct participation in hostilities hinges on their specific intent. If these measures are aimed at executing a particular hostile act, they fall within the purview of direct participation. However, when they serve to build a more general capacity for engaging in unspecified hostile acts, they do not meet the criteria for direct participation (Delerue 2014, 10). This distinction is crucial in defining the scope of actions that qualify as direct participation in hostilities under international humanitarian law.

The time-related aspect is challenging in the context of cyberspace due to the nature of cyber operations, encompassing their initiation, effects realisation, and termination (Schmitt 2010b, 16; Kilovaty 2016, 31). This is also complicated by the fact that some cyber operations may only reveal their consequences long after the civilian actor had reverted to their non-combatant status. The key challenge lies in dealing with the lasting effects of certain cyber operations. In essence, they blur the temporal boundaries of DPH. To address this, it is essential to establish a clear framework that distinguishes between the time when a civilian's involvement in cyber operations

renders them targetable under the DPH framework and the period when the enduring effects of those operations may still impact the target.

According to Kilovaty, it is important to differentiate between two types of sustained effects resulting from cyber operations (Kilovaty 2016, 31). There are cyber operations where the attack code remains active, leading to continuous consequences – the civilian conducting the cyber operation remains targetable as long as the DPH criteria are met when the code is operational (Dinnis 2012, 276). On the other hand, there are cyber operations that trigger prolonged effects, not directly linked to the ongoing cyber operation – the civilian may be considered targetable during the actual duration of the cyber operation (Dinnis 2012, 276).

Therefore, to effectively address the temporal challenges associated with cyber operations, a nuanced and context-specific approach is required, taking into account the evolving nature of cyber conflicts and the complex interplay between civilian actors, states, and their responsibilities in cyberspace. Navigating the temporal challenges inherent in cyberspace operations prompts a crucial consideration of the 'revolving door' concept and its applicability to cyber warfare. The swift and dynamic nature of cyberattacks, often detected after their execution, complicates the application of this concept.

7. THE REVOLVING DOOR CONCEPT

Civilians directly participating in hostilities do not cease to be part of the civilian population, but their protection against direct attack is temporarily suspended (Melzer 2009, 70).

The notion of the 'revolving door', which involves the loss and subsequent regaining of civilian protection for each specific act amounting to direct participation in hostilities, has generated considerable debate. It is considered customary international law according to the two additional protocols to the Geneva Conventions. However, experts involved in the Tallinn Manual process (the Tallinn Manual is not a binding international law instrument but "examines how extant legal norms apply to 'new' form of warfare") had varying opinions on this concept, and no consensus was reached (Schmitt 2013, 1).

The concept may initially appear valid and beneficial for evaluating liability in the context of cyberattacks, especially given their rapid and dynamic nature, although the application of the revolving door concept to cyber warfare is particularly challenging (Schmitt 2010b, 37–38). Cyberattacks are often quick to launch and execute, making it difficult to address the direct participation of the civilian due to their short duration of engagement. Additionally, many cyberattacks are only detected after they have been carried out, at which point the civilian perpetrators have already regained their civilian status, as per the existing legal framework.

These challenges raise significant questions about the adequacy of current legal frameworks in effectively addressing the dynamic and rapidly evolving landscape of cyber warfare.

In contrast, individuals who are considered "members of organised armed groups belonging to a non-state party to the conflict" undergo a different categorisation (Melzer 2009, 71). They lose their civilian status for the duration of their membership in such organised armed groups, as long as they continue to perform functions directly related to combat. This means that even if they are not actively engaged in hostile acts at a specific moment, their CCF keeps them from retaining civilian protection.

In brief, when a civilian engages in cyber operations irregularly and without a consistent pattern, they should have their civilian protection reinstated once the cyber operation ends. Nonetheless, if substantial evidence suggests their affiliation with hacking groups, their civilian protection might be revoked.

8. FINAL REMARKS

Cyberspace exists beyond the confines of physical war zones or specific geographic locations. In the realm of cyberspace, traditional notions of state territory become less relevant, giving rise to a virtual and universal landscape that is inherently complex to define (Hoffmann 2003, 419). Moreover, cyberspace thrives on anonymity, making it a haven for those engaged in cyberattacks who conceal their identities. However, the absence of clear identities poses a significant hurdle when it comes to assigning blame for these crimes to specific individuals, thereby impeding the process of holding them accountable. This challenge looms large over both domestic and international criminal jurisdictions.

A civilian hacker may be deemed to engage in direct participation in hostilities, thereby permitting the victim State to respond within the boundaries of international humanitarian law. Such a response would not qualify as a war crime. However, if the cyberattack predominantly disrupts civilian infrastructures and causes economic harm, the civilian hacker maintains their civilian status.[6] Consequently, any retaliatory action against them could potentially be construed as a war crime. The mentioned rule encompasses both armed forces members and civilians involved in cyber operations linked to ongoing armed conflicts while excluding those engaged in purely criminal or malicious cyber activities unrelated to the current international or non-international armed conflict.

Crucially, the protection provided by IHL ceases to apply if it is convincingly demonstrated that, through the cyberattack they initiated, the individual has

[6] See: The International Criminal Tribunal for the former Yugoslavia. *Prosecutor v. Galić (it-98–29).* Judgment of 5 December 2003, para 48.

engaged in direct participation in hostilities. Such a demonstration renders the individual a legitimate military target under the purview of IHL, allowing for a proportionate response. These complex legal dynamics are central to the article's exploration and offer insights into the evolving landscape of cyber warfare within the realm of international humanitarian law.

The primary purpose of the DPH framework is to serve as a mechanism for halting ongoing hostile actions rather than penalising individuals after the fact. As a result of breaches of international or domestic criminal laws, the individual responsible could still be subject to criminal prosecution (Fleck 2013, 255–257).

The legal status of civilian hackers is a complex phenomenon that requires a case-by-case analysis. Each cyber action may vary, and the legal evaluation depends on the specific details of the actions involved.

BIBLIOGRAPHY

Akande, Dapo. 2010. "Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities." *The International and Comparative Law Quarterly* 59(1): 180–192.

Buchan, Russell. 2016. "Cyber Warfare and the Status of Anonymous under International Humanitarian Law." *Chinese Journal of International Law* 15(4): 74–772.

Delerue, Francois. 2014. "Civilian Direct Participation in Cyber Hostilities." *IDP IDP Revista de Internet Derecho y Política* 19: 3–17.

Dinniss, Heather. 2012. *Cyber Warfare and the Laws of War. Cambridge Studies in International and Comparative Law*. Cambridge: Cambridge University Press.

Fleck, Dieter. Ed. 2013. *The Handbook of International Humanitarian Law*. 3rd ed. Oxford: Oxford University Press.

Henckaerts, Jean-Marie. Louise Doswald-Beck. 2005. *Customary International Humanitarian Law*. Geneva: International Committee of the Red Cross.

Hoffman, Michael. 2003. "The Legal Status and Responsibilities of Private Internet Users under the Law of Armed Conflict: A Primer for the Unwary on the Shape of Law to Come." *Washington University Global Studies of Law Review*: 415–426.

Kilovaty, Ido. 2016. "ICRC, NATO and the U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law." *Duke Law & Technology Review* 15: 1–38.

Lazar, Seth. 2013. "Necessity and non-combatant immunity." *Review of International Studies, British International Studies Association* 40(1): 53–76.

Longobardo, Marco. 2017. "(New) Cyber Exploitation and (Old) International Humanitarian Law." *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 77: 809–834.

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

Melzer, Nils. 2016. *International Humanitarian Law. A comprehensive introduction.* Geneva: International Committee of the Red Cross.

Prescott, Jody. 2012. "Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States?" 4th International Conference on Cyber Conflict (CYCON), Tallinn, Estonia, 5–8 June 2012.

Rodenhauser, Tilman, VIGANTI, Mauro. 2023. "8 rules for civilian hackers during war, and 4 obligations for states to restrain them." *Humanitarian Law and Policy*, October 4, 2023.

https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/

Schmitt, Michael. 2010a. "Deconstructing Direct Participation in Hostilities: The Constitutive Elements." *New York Journal of International Law and Politics* 42: 697–739.

Schmitt, Michael. 2010b. "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis." *Harvard National Security Journal* 1: 5–44.

Schmitt, Michael. 2013. *Introduction. In Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schmitt, Michael. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press.

Tidy, Joe. 2022. "Anonymous: How hackers are trying to undermine Putin." *BBC*, March 20, 2023. https://www.bbc.co.uk/news/technology-60784526

Tidy, Joe. 2023. "Meet the hacker armies on Ukraine's cyber front line." *BBC*, April 15, 2023. https://www.bbc.com/news/technology-65250356

Turns, David. 2012. "Cyber Warfare and the Notion of Direct Participation in Hostilities." *Journal of Conflict & Security Law* 17: 288–296.

Legal acts

International Committee Of The Red Cross, *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.

International Committee Of The Red Cross, *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.

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

International Committee Of The Red Cross, *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention),* 12 August 1949, 75 UNTS 287.

International Committee Of The Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, 1125 UNTS 3.

International Committee Of The Red Cross, *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.

Special Rapporteur on Extrajudicial, Summary Or Arbitrary Executions. 2010. *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Study on Targeted Killings*, UN Doc A/HRC/14/24/Add.6.

Supreme Court of Israel, *Public Committee against Torture in Israel v. Government of Israel (HCJ 769/02).* Judgement of 13 December 2006.

The International Criminal Tribunal for the former Yugoslavia. *Prosecutor v. Galić (it-98–29).* Judgment of 5 December 2003.