University of BRISTOL

Law Working Papers Series
Paper #004/2024

The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict

Dr Giacomo Biggio
University of Bristol Law School
Wills Memorial Building
Queen's Road
Bristol
BS8 1RJ

bristol.ac.uk/law/research/legal-research-papers

ISSN 2515-897X

The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict

Abstract

The armed conflict between Russia and Ukraine has been characterized by a considerable number of cyber operations by States and non-State actors in support to either party to the conflict. One year since the Russian invasion of Ukraine, the 'Russia-Ukraine cyber conflict' offers valuable insights for estimating the effectiveness of International Humanitarian Law in regulating the status and the conduct of individuals engaging in cyberspace operations during wartime. By discussing the status of hackers groups and individuals who have conducted cyber operations in support of Ukraine, this Article claims that the relevance of the concept of combatancy is diminished in the cyber domain, and that the notion of direct participation in hostilities must be adapted to the specific features of cyberspace. Furthermore, the article focuses on the issues relating to the targeting of individual who directly participate in hostilities by conducting cyber operations in support of Ukraine. By doing so, the Article argues that cyber direct participants place themselves at an increased risk of being attacked, even though the Russian armed forces are limited in their targeting decisions by the principles of proportionality and precaution.

Keywords: *Russia-Ukraine armed conflict; cyberwarfare; combatancy; direct participation in hostilities; distinction; military necessity; humanity; law of targeting; Cyber Partisans of Belarus; IT Army of Ukraine.*

Please cite as: Giacomo Biggio, 'The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict' (2024) 15:1 *Journal of International Humanitarian Legal Studies* 141-182.

Contents

Introduction

The armed conflict between Russia and Ukraine has been characterized by a considerable number of cyber operations by States and non-State actors in support to either party to the conflict. One year since the Russian invasion of Ukraine, the Russia-Ukraine cyber conflict offers valuable insights for estimating the effectiveness of International Humanitarian Law (IHL) in regulating the status and the conduct of individuals engaging in cyberspace operations during wartime.

By discussing the status of hacker groups and individuals who have conducted cyber operations in support of Ukraine, this article claims that the relevance of the concept of 'combatancy' is diminished in the cyber domain, and that the notion of direct participation in hostilities must be adapted to the specific features of cyberspace. Furthermore, the article focuses on the issues relating to the targeting of individual who directly participate in hostilities by conducting cyber operations in support of Ukraine. By doing so, the article argues that cyber direct participants place themselves at an increased risk of being attacked, even though the Russian armed forces are limited in their targeting decisions by the principles of proportionality and precaution.

The article is structured as follows. Section One defines the Russia-Ukraine cyber conflict, the relevant actors involved therein, and provides an outline of the relevant applicable principles and rules, namely the principle of distinction, the provisions on combatant status, and the notion of direct participation of hostilities (DPH). Section Two discusses the legal status of the Cyber Partisans of Belarus (CPB), a pro-Ukraine hacker group involved in the Russia-Ukraine cyber conflict to illustrate that several of the requirements of 'combatancy' must either be adapted to or have a diminished relevance in the cyber domain. The section will conclude that the CPB do not qualify as combatants.

Section Three then discusses the challenges that cyberspace poses to the notion of DPH, specifically on the threshold of harm and direct causation requirements, as well as the temporal loss of protection from attack that lasts 'for such time as' a civilian directly participates in hostilities. To demonstrate this statement, the notion of DPH will be assessed against specific acts of civilian participation.

Section Four discusses a hypothetical scenario involving the targeting of an individual direct participant who is sharing military intelligence through software and messaging applications, in order to assess the application of the principles of proportionality and precaution under the First Additional Protocol to the Geneva Conventions and customary IHL. More specifically, it will be shown that while the Russian armed forces must exercise a certain amount of restraint when making targeting decisions, direct participants are still at a tangible risk of being lawfully targeted.

Finally, Section Five provides a conclusion, highlighting the issues raised by such normative uncertainties.

1 The Russia-Ukraine Cyber Conflict

1.1 *The Russia-Ukraine Cyber Conflict and Pro-Ukraine Cyber Support*

The armed conflict between Russia and Ukraine began in February 2014,[1] when the Russian government occupied Crimea[2] in response to the Maidan revolution which forced the resignation of the Ukrainian President Viktor Yanukovych.[3] In parallel, Russia supported pro-Russian separatists of

[1] See generally Geneva Academy of International Humanitarian Law and Human Rights, 'International Armed Conflict in Ukraine' (*RULAC: Rule of Law in Armed Conflicts*, 28 March 2023) <https://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine#collapse1accord> accessed 29 March 2023 ('RULAC').

[2] Geneva Academy of International Humanitarian Law and Human Rights, 'Military Occupation of Ukraine by Russia' (*RULAC: Rule of Law in Armed Conflicts,* 12 January 2023) <https://www.rulac.org/browse/conflicts/military-occupation-of-ukraine#collapse2accord> accessed 29 March 2023;
Marie-Louise Gumuchian, Laura Smith-Spark, and Ingrid Formanek, 'Gunmen Seize Government Buildings in Ukraine's Crimea, Raise Russian Flag' (*CNN*, 27 February 2014) <http://edition.cnn.com/2014/02/27/world/europe/ukraine-politics/> accessed 29 March 2023.

[3] James Marson, Alan Cullison, and Alexander Kolandyr, 'Ukraine President Viktor Yanukovych Driven from Power', (*The Wall Street Journal,* 23 February 2014) <https://www.wsj.com/articles/SB10001424052702304914204579398561953855036> accessed 29 March 2023.

the Donetsk and Luhansk Peoples Republic against the Army of Ukraine[4] in a violent confrontation which escalated into armed conflict, extending throughout the Donbas region.[5]

From the beginning of the conflict, cyber warfare played an increasingly important role. In the years preceding the invasion of Ukraine on 24 February 2022, Russian governmental actors, such as the 'Sandworm' group, have allegedly been involved in several hostile cyber operations against Ukrainian governmental, military, and civilian infrastructures.[6] These included the NotPetya 'ransomware' attack,[7] which targeted Ukrainian governmental cyber-infrastructure and private companies before eventually spreading across several countries, causing an estimated ten billion dollars in losses in 2016.[8] The Russo-Ukrainian conflict also saw major acts of cyber-sabotage against essential civilian infrastructure[9] when parts of the Ukrainian power grid were shut down by the BlackEnergy and Industroyer malwares, in December 2015 and December 2016 respectively, which affected hundreds of thousands of civilians.[10]

---

[4] According to the RULAC analysis on the classification of the conflict, the protests in the Donbas turned into a non-international armed conflict in spring of 2014. Then, as Russia exercised 'overall control' on the republics of Donetsk and Luhansk since after the invasion of Ukraine, the conflict has turned into an international armed conflict in spring 2022. See RULAC (n 1). See also M N Schmitt, 'Ukraine Symposium – Classification of the Conflict(s) (*Articles of War*, 14 December 2022) <https://lieber.westpoint.edu/classification-of-the-conflicts/> accessed 1 April 2023; Robert Heinsch, 'Conflict Classification in Ukraine: The Return of the ''Proxy War''?' (2015) 91 ILS 323, 354-360.

[5] Mark Rachkevych, 'Armed Pro-Russian Extremist Launch Coordinated Attacks in Donetsk Oblast, Seize Regional Police Headquarters, Set Up Checkpoints', (*Kiev Post,* 12 April 2014) <https://www.kyivpost.com/article/content/war-against-ukraine/armed-pro-russian-extremists-seize-police-stations-in-donetsks-slavyansk-shaktarysk-fail-to-take-donetsk-prosecutors-office-343195.html> accessed 30 March 2023.

[6] The group is also known as unit 77455 within the GRU, that is, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. See Department of Justice, Office of Public Affairs, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace', (*The United States Department of Justice,* 19 October 2020) <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> accessed 30 March 2023. For a detailed discussion of the Sandworm group, see Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Random House 2019).

[7] A ransomware is a type of malicious software designed to block access to a computer until a sum of money is paid. See, 'What is Ransomware?' (*Kapersky*, n.d.) <https://www.kaspersky.com/resource-center/threats/ransomware> accessed 1 April 2023.

[8] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyber Attack in History' (*Wired*, 22 August 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world> accessed 1 April 2023.

[9] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (*Wired*, 3 March 2016) <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid> accessed 1 April 2023.

[10] Pavel Polityuk, Oleg Vukmanovic, and Steven Jewkes, 'Ukraine's Power Outage Was a Cyber Attack: Ukrenergo' (*Reuters*, 18 January 2017) <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA> accessed 1 April 2023; Kim Zetter, 'The Ukrainian Power Grid was Hacked Again', (*Vice,* 10 January 2017) <https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report> accessed 1 April 2023.

The alleged involvement of Russia has remained a constant after the invasion of Ukraine,[11] with cyber operations consisting in a combination of distributed denial-of-service (DDoS) attacks,[12] wipers,[13] and other malware,[14] the most noteworthy example being the hacking of the KA-Sat satellite network.[15] In parallel, an ever-growing number of cyber operations have been launched since 24 February 2022 by non-state actors in support of Ukraine, including the Cyber Partisans of Belarus (CPB), the IT Army of Ukraine (IT Army) and individual civilians.

For the purposes of this article, the analysis will focus solely on pro-Ukraine actors and cyber operations, whereas the legal issues raised by cyber operations allegedly launched by Russian agents and Russian-affiliated actors will not be discussed.

1.1.1 The Cyber Partisans of Belarus

The CPB is a collective of 'hacktivists' formed in September 2020, following a presidential election allegedly falsified by Alexander Lukashenko, the current president of Belarus. While the CPB initially targeted the Lukashenko regime,[16] they rose to prominence in late February 2022 by launching a ransomware attack which paralyzed the railway system of Belarus.[17] The attack was deployed as an

[11] See 'Cyber Attacks in Times of Conflict: Platform #Ukraine', (*Cyber Peace Institute*) <https://cyberconflicts.cyberpeaceinstitute.org/> accessed 1 April 2023.
[12] In this regard, a Denial of Service (DoS) attack is a cyber operation which is designed to disable the target network by flooding it with traffic. In a Distributed Denial of Service (DDoS) attack, multiple machines are operating together to flood the target network. See in this regard Heather Harrison Dinniss, *Cyberwarfare and the Laws of War* (Cambridge University Press 2012) 294; Cybersecurity & Infrastructure Security Agency (CISA), 'Understanding Denial-of-Service Attacks' (*CISA*, 1 February 2021) <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks> accessed 3 April 2023.
[13] A wiper is a type of malware (that is, malicious software) designed to erase data from the hard drive of the targeted computer. See Kaspersky IT Encyclopedia, 'Wiper' (*Encyclopedia by Kaspersky*) <https://encyclopedia.kaspersky.com/glossary/wiper/> accessed 3 April 2023.
[14] Laura Kelly, 'Ukraine Defense Ministry, Banks Hit by Cyberattack Amid Tensions With Russia', (*The Hill,* 15 February 2022) <https://thehill.com/policy/international/594330-ukraine-defense-ministry-banks-hit-by-cyberattack-amid-tensions-with/> accessed 3 April 2023; Dan Milmo, 'Russia Unleashed Data-Wiper Malware on Ukraine, Say Cyber Experts' (*The Guardian,* 24 February 2022) <https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts> accessed 3 April 2023.
[15] Viasat, 'Ka-sat Network Cyber Attack Overview' (*Viasat,* 30 March 2022) <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview> accessed 3 April 2023.
[16] Patrick Howell O' Neill, 'Hackers are Trying to Topple Belarus's Dictator, With Help From Others' (*MIT Technology Review,* 26 August 2021) <https://www.technologyreview.com/2021/08/26/1033205/belarus-cyber-partisans-lukashenko-hack-opposition/> accessed 3 April 2023.
[17] Andrew Roth, ''Cyberpartisans' Hack Belarusian Railway to Disrupt Russian Buildup' (*The Guardian,* 24 April 2022) <https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup> accessed 3 April 2023.

attempt to slow down Russian supply lines and disrupt the Russian army's military operations, since Russia had been using the Belarusian railway network in the northern front to transport troops and military equipment. Although the precise impact of the sabotage remains difficult to estimate, the CPB claimed that it was successful in slowing the movement of trains between Belarus and Ukraine.[18]

At the time of writing, the CPB are cooperating with the Kastus Kalinouski Regiment (KKR), a one thousand-strong battalion of Belarusian volunteers which forms part of the armed forces of Ukraine,[19] by sharing military intelligence related to the location of the Russian troops near the border between Belarus and Ukraine.[20]

1.1.2 The IT Army of Ukraine

The creation of the IT Army was announced on 26 February 2022 by a Tweet of Ukrainian Minister for Digital Transformation Mikhailo Fedorov, who called for IT specialists to help Ukraine 'fight on the cyber front'.[21] Fedorov's call for help rallied tremendous international support, with a reported 400,000 people joining the IT Army within the first week of its establishment[22]. In the days, weeks, and months that followed, the IT Army has claimed responsibility for an array of cyber operations directed against Russian targets, including the Moscow Stock Exchange and Russian bank

---

[18] Joel Schectman, Christopher Bing, and James Pearson, 'Ukrainian Cyber Resistance Group Targets Power Grid, Railways' (*Reuters,* 1 March 2022) <https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/> accessed 3 April 2023.

[19] 'The Kastus Kalinouski Regiment' (*The Kastous Kalinouski Regiment*) <https://kalinouski.org/en/about> accessed 3 April 2023.

[20] Dominic Culverwell, 'INTERVIEW: "Without a Free Ukraine, There is No Chance for a Free Independent Belarus' Says Hacktivists Belarusian Cyber Partisans' (*Intellinews,* 9 July 2022) <https://www.intellinews.com/interview-without-a-free-ukraine-there-is-no-chance-for-a-free-independent-belarus-say-hacktivists-belarusian-cyber-partisans-250026/> accessed 3 April 2023.

[21] Mikhailo Fedorov, 'We Are Creating an IT Army' (*Twitter*, 26 February 2022) <https://twitter.com/fedorovmykhailo/status/1497642156076511233?lang=en> accessed 3 April 2023.

[22] Sam Schechner, 'Ukraine's 'IT Army' Has Hundreds of Thousands of Hackers, Kyiv Says' (*The Wall Street Journal*, 4 March 2022) <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX> accessed 3 April 2023.

Sberbank,[23] as well as launching DDoS attacks against several civilian targets such as pharmacies and ATM machines.[24]

1.1.3 Other Forms of Pro-Ukraine Cyber Support

Alongside the involvement of hacker groups and collectives, the Russia-Ukrainian cyber conflict has been characterized by the participation of individual civilians who have supported Ukraine by downloading and using government sponsored applications and software. These include 'eVorog' ('E-Enemy' in Ukrainian'),[25] a Telegram chat where users can transmit the location of Russian troops weapons and other military equipment to the Ukrainian army by uploading video and photographic evidence, and 'ePPO',[26] a mobile app specifically designed to signal the presence of Russian cruise missiles and kamikaze drones to the Ukrainian air defense system.

1.2 *Scope of Application of IHL*

Before discussing the legal status of pro-Ukraine hackers under the *jus in bello*, it is necessary to clarify the extent to which IHL applies to the Russo-Ukraine war and the specific principles and provisions relevant for the analysis. The Russia-Ukraine conflict qualifies as an International Armed Conflict (IAC) to which IHL applied from the moment Russia annexed Crimea in February 2014.[27]

---

[23] Thomas Brewster, 'Moscow Exchange, Sberbank Websites Knocked Offline – Was Ukraine's Cyber Army Responsible?' (*Forbes*, 28 February 2022) <https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=5dda2477cae3>.

[24] Stefan Soesanto, 'CYBERDEFENSE REPORT The IT Army of Ukraine Structure, Tasking, and Ecosystem' (*ETH Zurich Centre for Security Studies,* June 2022) https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf; L. Franceschi-Bicchierai, 'Inside Ukraine's Decentralized Cyber Army' (*VICE,* 19 July 2022) <https://www.vice.com/en/article/y3pvmm/inside-ukraines-decentralized-cyber-army>.

[25] Drew Harwell, 'Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War' (*The Washington Post*, 24 March 2022) <https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/> accessed 1 May 2023; 'Ministry of Digital Transformation Launches eVorog Chatbot in Telegram' (*Interfax-Ukraine,* 10 March 2022) <https://en.interfax.com.ua/news/telecom/810765.html> accessed 1 May 2023.

[26] 'Using the ePPO Application, Ukrainians can Help Anti-Aircraft Fighters Shoot Down Enemy Drones and Missiles' (*The Main Directorate of Intelligence of the Ministry of Defense of Ukraine,* 13 October 2022) <https://gur.gov.ua/content/ukraintsi-cherez-zastosunok-ieppo-mozhut-dopomohty-zenitnykam-zbyvaty-vorozhi-drony-ta-rakety.html> accessed 1 May 2023; Dan Sabbagh, 'Ukrainians use Phone App to Spot Deadly Russian Drone Attacks' (*The Guardian,* 29 October 2022) <https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo> accessed 1 May 2023.

[27] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (First Geneva Convention) Common Article 2.

In this regard, the distinction between international and non-international armed conflicts (NIACs) results in the application of two different legal regimes. Despite the development of customary IHL, which has led to significant similarities in the applicable rules,[28] one essential difference which persists is the concept of 'combatancy', which is exclusive to IACs.[29]

The concept of combatancy is a logical corollary to the 'intransgressible' principle of distinction between civilians and combatants.[30] Combatancy performs the fundamental function of ensuring a balance between military necessity and humanity,[31] the two normative driving forces or meta-principles,[32] that underly modern IHL.[33] The principle of military necessity permits a belligerent to employ any measure which is deemed necessary for securing a military objective and is not otherwise prohibited by law.[34] In other words, it legitimizes the use of armed force and the causation of death, injury or destruction as long as it is instrumental for the accomplishment of a lawful military purpose.

While the principle of military necessity is permissive in nature,[35] the principle of humanity, as firstly referenced in the Martens Clause,[36] performs a restrictive function within IHL, thereby limiting the

[28] See in this regard Jean-Marie Henckaerts and Louise Doswald-Beck (eds.) *Customary International Humanitarian Law* (Cambridge University Press 2005) ('Customary IHL'); Noam Zamir, *The Classification of Conflicts in International Humanitarian Law* (Edward Elgar 2017) 74; Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (Oxford University Press 2012) 230.
[29] ibid Volume I, Ch. 33 p 384.
[30] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) ICJ Reports 1996, 226 [78]-[79].
[31] Michael Schmitt, 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance' (2010) 50 VJIL 795, 798.
[32] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022) 50; B. J. Bill, 'The Rendulic 'Rule': Military Necessity, Commander's Knowledge, and Methods of Warfare' (2009) 12 YIHL112, 131, defining military necessity as a 'meta-principle of the law of war' permeating all rules.
[33] Dieter Fleck, 'Humanitarian Requirements and Military Necessity' in Dieter Fleck (ed.) *The Handbook of International Humanitarian Law* (4th edn, Oxford University Press 2021) 42-45.
[34] Francis Lieber, *Instructions for the Government of Armies of the United States in the Field* (United States War Department 1898); *United States v List (Hostages Trial)* (1948) 11 TWC 757.
[35] Anne Quintin, *The Nature of International Humanitarian Law* (Edward Elgar 2020) 30; Lawrence Hill-Cawthorne, 'The Role of Necessity in International Humanitarian and Human Rights Law' (2014) 47 Israel Law Review 225, 232–234.
[36] *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, 18 October 1907, Preamble: 'Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience.' For the purposes of this article, the terms 'principle of humanity', 'humanitarian considerations' and 'humanitarian concerns' will be used interchangeably.

amount of violence than can be lawfully deployed in the battlefield.[37] The balance between the principles of military necessity and humanity is operationalized by the rules of targeting under Additional Protocol I (AP I) and customary IHL. These rules are comprised of the principles of distinction, proportionality, and precaution. While the latter principles will be discussed *infra*,[38] the principle of distinction requires belligerents to distinguish between civilians and combatants at all times and to direct their military operations solely against military objectives.[39]

Individuals belonging to the combatant category enjoy 'the right to lawfully participate in hostilities',[40] from which several consequences arise. First, combatants are liable to be targeted for the duration of the conflict by virtue of their status. Second, combatants cannot be criminalized under domestic law for having committed lawful acts of war. Third, combatants are granted the status of 'prisoner of war' (POW) and related rights upon capture, as provided by the Third Geneva Convention (GCIII).

At the opposite end of the spectrum are civilians, who enjoy absolute protection from attack, unless and for such time as they take a direct part in hostilities.[41] Civilians have no right to lawfully participate in hostilities: as such, upon capture they are not considered POWs but, instead, are within the scope of application of the Fourth Geneva Convention (GCIV). Therefore, the determination of who is a civilian and who is a combatant has important implications for targeting decision and for the granting of POW status.

1.2.1 The Normative Framework on Combatant Status

To proceed with the analysis, it is necessary to identify which rules regulate combatant status. According to Art 43(2) of the AP I, combatants are all members of the armed forces of a Party to the

[37] Jens David Ohlin and Larry May, *Necessity in International Law* (Oxford University Press 2016) 183-184; Schmitt (n 31) 799.
[38] See Section Four.
[39] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1979) 1125 UNTS 3 ('AP I') Art 48.
[40] ibid art 43(2).
[41] bid art 51(3).

Conflict.[42] In turn, the term 'armed forces' is defined by Art 43(1) of the AP I as 'all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates'.[43] Both definitions reflect customary IHL.[44]

According to Art. 4(A)(1) of the GCIII, combatant status is granted to the armed forces of a State, including members of militias and volunteer forces which are part of such armed forces.[45] Moreover, 'members of other militias and volunteer corps' also qualify as combatants,[46] provided they meet the conditions provided by Art 4(A)(2) of the GCIII: being under responsible command, having a fixed distinctive emblem recognizable at a distance, carrying arms openly,[47] and conducting their operations in accordance with the laws and customs of war.[48] In addition to the above, two more conditions can be implied from Art 4(A)(2) of the GCIII, namely belonging to a party to the conflict and being organized.[49]

An additional category is that of a *levee en masse*, defined by Art 4(A)(6) of the GCIII as follows:

> '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 rules and customs of war.'[50]

Combatant status is further regulated by Additional Protocol I, which introduced slight differences compared to Art 4 of the GCIII. Firstly, Art 43(1) of the AP I removed the distinction between 'regular' and 'irregular' armed forces provided by Arts 4(1)(A) and 4(2)(A) of the GCIII, respectively. According to Knut Ipsen, both categories now fall within the meaning of 'organized armed forces,

---

[42] AP I (n 39) art 43(2).
[43] ibid art 43(1).
[44] *Customary International Humanitarian Law* (n 28) Rule 3.
[45] Geneva Convention Relative to the Treatment of Prisoners of War (12 August 1949) 75 UNTS 135 ('GCIII') art 4(A) This category will be referred to as 'regular armed forces'.
[46] This category will be referred to as 'irregular armed forces'.
[47] For the purposes of this Article, the two requirements will be also referred to as 'requirements of distinction'.
[48] GCIII (n 45) art 4(A)(2).
[49] Dinstein (n 32) 59.
[50] GCIII (n 45) art 4(A)(6).

groups and units which are under a command responsible to that Party for the conduct of its subordinates'.[51]

Secondly, Art 43(1) of the AP I adds that organized armed forces, groups and units 'shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict.'[52] In this sense, the definition of 'armed forces' given by Art 43(1) of the AP I reaffirms four of the six requirements of combatant status: organization, responsible command, belonging to a Party to the conflict, and compliance with IHL.[53]

Thirdly, Art 44(3) of the AP I provides an exception to the requirements of distinction in situations where a combatant cannot distinguish himself from the civilian population 'due to the nature of hostilities', phrasing which applies to guerrilla fighting in times of occupation and in wars of national liberation.[54] In such a situation, a combatant must carry his arms openly 'during each military engagement' and 'during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.'[55]

For the purposes of this Article, since both Russia and Ukraine are parties to the AP I, the legal status of pro-Ukraine hacker groups will be examined by reference to Art 43 of the AP I.

---

[51] Knut Ipsen, 'Combatants and Non-combatants' in Dieter Fleck (ed.) *The Handbook of International Humanitarian Law* (4th edn, Oxford University Press 2021) 100, [5.04].
[52] AP I (n 39) art 43(1).
[53]Yves Sandoz, Catherine Swinarski and Bruno Zimmermann (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nihjoff 1987) 517, [1681]: 'To summarize: ' the conditions which should all be met to participate directly in hostilities are the following: a) subordination to a "Party to the conflict" which represents a collective entity which is, at least in part, a subject of international law; b) an organization of a military character; c) a responsible command exercising effective control over the members of the organization; d) respect for the rules of international law applicable in armed conflict. These four conditions should be fulfilled effectively and in combination in the field.'
[54] ibid [1698].
[55] AP I (n 39) art 44(3).

2 The Russia-Ukraine Cyber Conflict and the Requirements of 'Combatancy' in the Cyber Domain: the Status of the Cyber Partisans of Belarus

Our discussion begins with two premises. Firstly, given the lack of information available on the structure and composition of the IT Army,[56] this article will assume that they should be considered civilians who may commit acts amounting to DPH. Therefore, this section will be exclusively concerned with discussing the legal status of the CPB.[57] Secondly, because the rules on combatancy are the result of a normative process aimed at regulating the physical battlefield, the greatest interpretive challenge is clarifying how these rules can be adapted to the cyber domain. This will be explored with the constitutive elements underpinning the notion of 'armed forces' under Art 43 of the AP I: the meaning of 'armed', the requirements of organization, responsible command, compliance with IHL, and belonging to a Party to the conflict. Then, the focus of the discussion will shift to the interpretive challenges raised by the requirements of distinction, before offering a provisional conclusion.

2.1 *Hacker Groups, the Cyber Domain, and the Meaning of 'Armed Forces' Under Art 43 AP I*

The term 'armed forces' under Art 43 of the AP I includes 'all organized armed forces, groups and units which are under a command responsible to a Party for the conduct of its subordinates.' To determine if the CPB fall within the meaning of 'armed forces', it should be noted that the notion of 'armed' is connected to how the term 'attack' in understood in contemporary IHL.[58]

---

[56] See Soesanto (n 24). For an examination of the legal status of the IT Army, see Russell Buchan and Nicholas Tsagourias, 'Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?' (*EJIL: Talk!,* 9 March 2022)<https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/> accessed 3 April 2023; Casey Biggerstaff, 'The Status of Ukraine's "IT Army" under The Law Of Armed Conflict' (*Articles of War,* 10 May 2023) <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/> accessed 13 May 2023.

[57] This Article assumes that the CPB do not qualify as individuals participating in a *levee en masse*. For an analysis on how the concept applies to the cyber domain, see David Wallace and Shane Reeves, 'The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare' (2013) 89 ILS 646.

[58] Michael Schmitt, 'Cyber Operations and the *Jus in Bello*: Key Issues' (2013) 87 ILS 89, 99-100 ('Key Issues'), noting that 'the reach of the adjective "armed" depends on the interpretation adopted vis-à-vis the term "attack."'.

Currently, there is no consensus on how the notion of attack should be applied in the cyber domain. One view, exemplified by the position adopted by the *Tallinn Manual*, is modeled after the wording in Art 49 of the AP I, which defines attacks as 'acts of violence against the adversary, whether in offence or defence'.[59] Consequently, the *Tallinn Manual* argues that any 'cyber operation that is reasonably expected to cause death or injury to individuals, or damage or destruction to objects' qualifies as an attack under IHL.[60] This approach, also referred to as the 'kinetic-equivalence effects test' (KEE test),[61] is premised upon the causation of physical violence, akin to that caused by kinetic weapons. Any other cyber operation that results in a different kind of violence, be it economic or psychological,[62] is not an attack.[63]

While the KEE test has been endorsed by States like Australia,[64] Israel,[65] the United Kingdom,[66] and the United States,[67] its suitability has been questioned on the basis that it excludes cyber-operations causing severe disruptive consequences not amounting to physical violence.[68] For example, the cyber-attacks against the Ukrainian power grid would not be considered an 'attack' under the KEE test, as it did not result in death or injury to individuals or damage and destruction to objects. Therefore, a hacker group that engages in such kind of cyber operations would not be deemed as 'armed' under

---

[59] AP I (n 39) art 48.
[60] Michael Schmitt (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyberspace Operations* (Cambridge University Press 2017) 415, Rule 92 ('Tallinn Manual 2.0'): Michael Schmitt (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 106, Rule 30 ('*Tallinn Manual 1.0'*).
[61] Carine Bannelier-Kristakis, 'Is the Principle of Distinction Still Relevant in Cyberspace?' in Nicholas Tsagourias and Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 343, 348.
[62] In this regard, it is worth noting that the *Tallin Manual 2.0* extends the definition of 'attack' to serious illness or mental suffering that are tantamount to injury. See *Tallinn Manual 2.0* (n 61) 417.
[63] *Tallinn Manual 2.0* (n 61) 418, discussing the qualification of a cyber operation that does not cause physical violence, but results in large-scale adverse consequences.
[64] Australian Government, *Australia's Position on how International Law Applies to State Conduct in Cyberspace* (*Australian Government*, 2021) <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>.
[65] Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 ILS 395, 400.
[66] Foreign, Commonwealth and Development Office, *Application of International Law to States Conduct in Cyberspace: UK Statement.* (*UK* Government) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement>.
[67] United States Department of Defense, *Law of War Manual* (2016) 1012 ('US Law of War Manual').
[68] See Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians' (2012) 886 International Review of the Red Cross 94 533, 557; Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 ILS 252, 264; Bannelier-Christakis (n 61) 348-353.

Art 43 of the AP I.[69] Absent this precondition, any discussion on the requirements of combatant status would not be necessary, since members of such a group would be considered as civilians who may (or may not) commit acts amounting to DPH.

Among the alternative approaches to the KEE test,[70] the position taken by the International Committee of the Red Cross (ICRC) considers an attack any cyber operation that is designed to disable the functionality of a computer or computer network.[71] This interpretation has been supported, *inter alia*, by France,[72] Japan,[73] and New Zealand.[74] An even more expansive approach has been adopted by Germany, which holds that the notion of attack should include any 'act or action initiated in or through cyberspace which is capable of causing harmful effects'. [75]

In the opinion of the present author, the main weakness of these views is that they do not provide any *de minimis* threshold as to what constitutes an attack in the cyber domain. In fact, if all that is required is disabling the functionality of the target computer network or system, it follows that cyber operations causing mere inconvenience, such as a DDoS attack, would be considered as attacks.[76] In practice, a

---

[69] Unless such a hacker group has been formally incorporated in the armed forces of a State party to an IAC. Interestingly, such is the case of the Sandworm group, the threat actor allegedly responsible for NotPetya and the cyber attacks against the Ukrainian power grid in 2015 and 2016.

[70] See, for instance, Giacomo Biggio, 'International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I' (2021) 59(1) The Military Law and the Law of War Review 114; David Wallace and Shane Reeves, 'Protecting Critical Infrastructure in Cyber Warfare: Is It Time for States to Reassert Themselves?' (2020) 53 University of California Davis Law Review 1618. Ido Kilovaty, 'Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law' (2016) 23(1) Michigan Telecommunication and Technology Law Review 113; Bannelier-Christakis (n 61); Marco Roscini, *Cyber Operations and the Use of Force under International Law* (Oxford University Press 2014) 181.

[71] ICRC*, International Humanitarian Law and Cyber Operations During Armed Conflict: ICRC Position Paper* (*ICRC,* November 2019) 7-8 <https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf> accessed 3 April 2023.

[72] Ministere Des Armees, '*Droit International Applique Aux Operations Dans Le Cyberspace'* (*Republic of France*, 2019) 13 <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.> accessed 3 April 2023.

[73] Ministry of Foreign Affairs, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (*Ministry of Foreign Affairs Japan*, 16 June 2021) 7 <https://www.mofa.go.jp/files/100200935.pdf> accessed 3 April 2023.

[74] 'The Application of International Law to State Activity in Cyberspace' (*New Zealand Government*, 1 December 2020) [25]<https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> accessed 26 April 2023.

[75] *On the Application of International Law in Cyberspace* (The Federal Government of Germany, March 2021) 8 <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pd> accessed 3 April 2023.

[76] Droege (n 68) 559.

group of hackers like the IT Army, which primarily conducts such kind of cyber operations, would be regarded as 'armed' and, provided that they satisfy the requirements for combatancy, be granted combatant status and be liable to be targeted at all times. This is an unsatisfactory legal outcome, as members of such a hacker group should instead be regarded as civilians who may commit acts of DPH.[77]

In this regard, it is submitted that a more balanced approach should look at the intensity and significance of the consequences of a given cyber operation. Therefore, the notion of attack in the cyber domain should include not only cyber operations causing physical violence, but also those resulting in large-scale adverse consequences,[78] such as severe economic losses, severe disruption of essential civilian services, or a combination thereof.[79] In addition, cyber operations resulting in military harm, as the concept is defined in the *Interpretive Guidance to the Notion of Direct Participation in Hostilities*,[80] should also qualify as attacks.[81]

Under this interpretation, the CPB can be considered as 'armed' for the purposes of Art 43 of the AP I, because they have engaged in cyber operations. These resulted in military harm by deploying ransomware against the railway network of Belarus, and also by repeatedly sharing military intelligence with the KKR, in order to enable the former to target the Russian armed forces.[82]

2.2 The Requirements of Organisation and Responsible Command

Both the requirements of organization and responsible command flow from the same *rationale* of discouraging individuals from waging a war on their own, instead of joining an organized armed

[77] See *infra*, Section 3.2.1 for a discussion on whether the cyber operations launched by the IT Army amount to DPH.
[78] The inclusion of cyber operations causing large-scale adverse consequences not amounting to death, injury or destruction as attacks has been considered by the *Tallinn Manual*. In this regard, while the majority of experts took the position that 'the law of armed conflict does not presently extend this far', the minority took the position that 'took the should an armed conflict involving such cyber operations break out, the international community would generally regard them as attack'. See *Tallinn Manual 2.0* (n 60) 418.
[79] Biggio (n 70) 138-140.
[80] Nils Melzer, *Interpretive Guidance to the Notion of Direct Participation in Hostilities* (*ICRC,* 2009) ('DPH Guidance').
[81] For a discussion of the concept of 'military harm', see *infra*, Section 3.1.
[82] See *infra* Section 3.2.2.

group or the armed forces of a State.[83] In other words, their aim is to 'keep rogue actors from the rubric of war'.[84] Albeit in the context of a NIAC, [85] the two requirements have been interpreted by international criminal tribunals in a way that accounts for the existence of different degrees and types or organization and command structure. [86] This is evidenced in *Akayesu*, where the International Criminal Tribunal for Rwanda (ICTR) found that a sufficient level of organization and responsible command constitutes the means 'to enable the armed group or dissident armed force to plan and carry out concerted military operations, and to impose discipline in the name of a *de facto* authority.'[87]

Furthermore, in *Boskoski and Tarculovski*, the International Criminal Tribunal for the former Yugoslavia (ICTY) provided a list of indicative factors of organization and responsible command. The first factor is if the group has a command structure, which includes the establishment of a general staff or high command that appoints and gives directions to commanders, organizes the weapon supply, authorizes military action, and authorizes individuals in the organization. Then, the Court included factors that indicate that the group can carry out organized operations, such as control over territory, logistical capabilities like the provision of military training and the recruitment of new members. The list included factors that indicate that the group possesses a level of discipline, such as the establishment of disciplinary rules and mechanisms. Lastly, the ICTY looked at the ability of the group to speak with one voice, evidenced by the capacity to speak on behalf of its members in political negotiations.[88]

Certain factors, such territorial control, the existence of headquarters, or the supply and use of uniforms, have been designed to apply to the physical battlefield and cannot be analogized to the

[83] Sandoz. Swinarski, and Zimmerman (n 53), 512; Russell Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' (2016) 15(4) Chinese Journal of International Law 741, 748.
[84] Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50(2) Virginia Journal of International Law 437.
[85] Buchan (n 83) 748; *Tallinn Manual 2.0* (61) 98, Rule 26. When discussing the concept of organization as a requirement for POW status, the Commentary to Rule 26 notes that 'The criterion of organization was
previously discussed in the context of non-international armed conflict (Rule 23). There, the unique nature of virtual organizations was highlighted. The same considerations apply in the present context.'
[86] See also Sandoz, Swinarski, and Zimmerman (n 53) 521.
[87] *Prosecutor v Jean-Paul Akayesu* (Trial Judgement) ICTR-96-4-T, [626].
[88] *Prosecutor v Ljube Boskoski and Johan Tarculovski* (Judgment) IT-04-82-T, [199]-[203].

cyber scenario, as they would be irrelevant due to the decentralized and virtual nature of cyberspace. That said, others can be transposed to the cyber context or 'cyberized': consider the provision of training and recruiting new members, the ability to speak with one voice, or having a hierarchical structure where decisions are taken in relation to the choice of cyber operations, their targets, and their execution.

In principle, there is nothing that prevents a group of hackers from satisfying the requirement of being organized, since the group can be virtually organized, and all its activities may take place online. On the other hand, the requirement of being under responsible command appears difficult to satisfy in the cyber domain, as there would be no means to implement an internal disciplinary system capable of enforcing compliance with IHL in relation to individuals with whom there is no physical contact.[89]

Do the CPB satisfy the requirements of organization and responsible command? To begin with, they have an official spokeswoman, Yuliana Shemetovets, through whom they share information relating to their political motives and their organizational structure.[90] In this regard, the CPB are one of the three founding members of a larger Belarusian anti-government resistance movement, known as 'Supratiⅴ', and numbered around 30 active members at the beginning of 2022.[91] While the vast majority of their members were Belarusian citizens working in the IT community, since the Russian invasion of Ukraine the group has reportedly grown in numbers, accepting individuals from different countries.[92]

Despite no information being released as to exact location of the CPB headquarters, it is safe to infer that the CPB appear to be more than a loosely-tied group of individuals scattered around the globe,

[89] In this regard, see *Tallinn Manual 2.0* (n 61) 390, 405. For a critique of the requirement in the cyber domain, see Watts (n 84) 441-442.
[90] Ylenia Gostoli, 'How I Became the Spokesperson for a Secretive Belarusian 'Hacktivist' Group' (*TRT World,* 10 February 2022) <https://www.trtworld.com/magazine/how-i-became-the-spokesperson-for-a-secretive-belarusian-hacktivist-group-54617> accessed April 2023.
[91] Max Smeets and Brita Achberger, 'Cyber Hacktivists are Busy Undermining Putin's Invasion' (*The Washington Post*, 13 May 2022) <https://www.washingtonpost.com/politics/2022/05/13/cyber-attack-hack-russia-putin-ukraine-belarus/> accessed 27 April 2023.
[92] Gostoli (n 90).

united by a common goal, such as the Anonymous collective.[93] Furthermore, the group appears to operate on a basic hierarchical structure, since only 'a core of three to five members' is responsible for conducting offensive cyber operations, while the rest are tasked with activities such as developing, testing, or analysing data.[94] Thus, it can be submitted that the CPB are sufficiently organized for the purposes of Art 4(A)(2) of the GC III. On the other hand, there is insufficient evidence to argue that there is a command structure within the CPB, and that its members are under responsible command.

2.3 *Compliance with IHL*

In relation to the requirement of compliance with IHL, what must be assessed is the level of compliance of the group as a whole, and not that of the individual.[95] As such, individual members of an armed group would not qualify as lawful combatants if the activities of the group do not meet the requirement.[96] The primary example of conduct not in compliance with IHL would be violating the principle of distinction by intentionally targeting the civilian population, civilian objects, as well as individuals and objects who enjoy protected status.[97]

In the case of the CBP, the ransomware attack launched against the Belarusian Railways targeted only those parts of the network that were used by Russia to transport its troops from the Belarusian border to Ukraine, whereas civilian routes were intentionally left unaffected. The cyber-operation thus complies with the principle of distinction. The same conclusion can be drawn in relation to the cyber operations aimed at gathering intelligence related to the position of the Russian troops, which is then

---

[93] Parmy Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency* (Cornerstone 2013) 68.
[94] Gostoli (n 90).
[95] Dinstein (n 32) 62; Knut Dormann et al (eds.), *Commentary to the Third Geneva Convention* (Cambridge University Press 2021) 376; Howard Levie, 'Prisoners of War in International Armed Conflict' (1977) 59 ILS 52.
[96] G Draper, 'The Status of Combatants and the Question of Guerilla Warfare' (1973) 45 British Yearbook of International Law 173, 197; Theodor Meron, 'Some Legal Aspects of Arab Terrorists' Claims to Privileged Combatancy' (1970) 40 Nordisk Tidsskrift for International Ret 47, 65. *Contra*, Dinstein (n 32) 68.
[97] This would include, for instance, the obligation not to direct attack against medical personnel, and persons and objects displaying the distinctive emblem. See *Customary International Humanitarian Law* (n 28) 30, Rule 25; ICRC, *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems*: *Benefits, Risks, and Possible Solutions* (*ICRC*, 2022) <https://www.icrc.org/en/document/icrc-digital-emblems-report> accessed 10 May 2023.

communicated to the KKR to enable them to carry out their attacks. Therefore, the compliance requirement appears to be satisfied.

2.4 *The Requirement of Belonging to a Party to the Conflict*

According to the ICRC, the requirement of belonging to a Party to the Conflict requires a '*de facto* relationship between the resistance organization and the party which is in a state of war, but the existence of this relationship is sufficient.'[98] Two conditions must be met to satisfy the criterion, namely that the group is fighting on behalf of a Party to the conflict and that the Party accepts 'both the fighting done by the group and the fact that the fighting is done on its behalf' either expressly or tacitly.[99]

The CPB expressed support to the Ukrainian cause on at least on two different occasions. On 24 February, the CPB's spokesperson Tweeted that 'Ukrainian and Belarusians have a common enemy – Putin, the Kremlin, the imperial regime'.[100] More recently, in July 2022, she stated, 'without a free Ukraine, there is no chance for a free independent Belarus. That is why the CPB are now doing everything possible to help Ukrainians.'[101] However, the Ukrainian government has not made any public statement on the matter. In the absence of any other form of approval or endorsement by the Ukrainian government,[102] its silence cannot be construed as a form of tacit acceptance of the support expressed by the CPB. Therefore, the CPB do not satisfy the requirement of 'belonging to a party to the conflict'.

2.5 *The Cyber Domain and the Diminished Relevance of the Requirements of Distinction*

Both the requirements of 'wearing a fixed distinctive emblem recognizable at a distance' and 'carrying arms openly' operationalize the principle of distinction between civilian and combatants.

---

[98] Jean Pictet, *Commentary on the Third Geneva Convention* (*ICRC*, 1960) 57; *DPH Guidance* (n 80) 23.
[99] Dormann (n 95) [1004]-[1007] and related examples.
[100] Yuliana Shemetovets, 'Ukrainian and Belarusians Have a Common Enemy' (*Twitter*, 24 February 2022) <https://twitter.com/yuliana_shem/status/1496719545389752321?>
[101] Culverwell (n 20).
[102] See Dormann (n 95) 1007, fn 118.

Regrettably, their scope of application to the cyber domain is greatly diminished, especially with regards to the requirement of carrying arms openly.

In relation to the requirement of wearing a fixed distinctive emblem, there is a certain degree of flexibility involved in the construction of the provision.[103] This means that the assessment on whether a combatant is 'wearing a fixed distinctive emblem' is necessarily context specific. In situations of spatial and temporal proximity to the area where hostilities are taking place, it is necessary for combatants to distinguish themselves from the population by wearing uniforms recognizable at a distance in order not to be mistaken for civilians. Conversely, there are instances in which the requirement must be assessed more leniently: as such, combatants are not obliged to wear a fixed distinctive emblem when they operate in areas outside the combat zone or when they are off duty.[104]

In the cyber domain, only members of a hacker group that operate in close proximity with the physical battlefield should be under the obligation comply with the requirement.[105] Should members of the CPB operate near an area of active hostilities, they would be required to wear a fixed distinctive emblem. Considering, however, that cyber warfare is performed remotely and in anonymity, this appears to be an unlikely scenario.

Regarding the requirement of open carriage of arms, its literal application leads to unrealistic outcomes.[106] Since cyber-weapons are nothing more than strings of code which are deployed on the target system (or server) using various techniques, carrying arms openly in cyberspace would require absolute transparency from the attacker in relation to their cyber-weapon of choice. In practice, this

[103] Dinstein (n 32) 61, noting that 'The formulation of the condition of wearing a fixed distinctive emblem in battle raises a number of questions. It is not easy to fathom the requirement that the distinctive emblem must be recognizable at a distance. The phraseology needs to be reasonably construed.'
[104] Toni Pfanner, 'Military Uniforms and the Law of War'(2004) 853 International Review of the Red Cross 93 101.
[105] Dinniss (n 12) 148. *Contra*, see *Tallinn Manual 2.0* (n 61): 'Combatant status requires that the individual wear a 'fixed distinctive sign'. The requirement is generally met through the wearing of uniforms. There is no basis for deviating from this general requirement for those engaged in cyber operations.'
[106] *Tallinn Manual 1.0* (n 61)100. See also Watts (n 84) 440.

would require the CPB to disclose the source code of the ransomware attack they employed against the Belarusian railway network.

This would create several issues. For instance, the code can be employed by other hackers against different targets. Moreover, it could undermine the effectiveness of the attack itself, as the greatest advantage of a cyber-weapon lies in its surprise factor: once the code of a virus is revealed, it becomes possible to adopt measure to mitigate its impact, for example by patching previously unknown vulnerabilities within the system of the Belarusian railway network. The same consideration can be drawn in relation to the exception provided by Art 44(3) of the AP I. Even assuming that the provision can be applied to cyber operations,[107] its wording is hard to reconcile with the reality of cyber warfare. Cyber operators are not 'visible by the adversary', and each 'military engagement' and 'military deployment' is carried out in complete anonymity.

Additionally, there have been several attempts at 'cyberizing' the requirement, for instance by suggesting that every cyber attack must originate from a designated IP address.[108] While this would simplify the issue of attributing the cyberattack to a hacker group, it has been noted that 'requiring a computer to be marked as a military computer is tantamount to placing a target on any system to which it is connected.'[109] If hacker groups are obliged to launch their cyber attacks from a designated IP address, they would be immediately identifiable and easily targeted through cyber and kinetic means. Given that anonymity and secrecy are essential to how hacker groups operate, this raises doubts as to the potential level of compliance with this requirement.

---

[107] Dinniss (n 12) 149. The author notes when discussing Art 44(1) of the AP I that, 'The controversial provision is aimed primarily at guerrilla fighters, whose use of covert tactics are designed to address inequality between the military and logistical means of the parties. However, an argument can be made that computer network attacks are an example of a type of warfare, the nature of which is anticipated by this provision. Computer network attacks are by their very nature a covert method of warfare…'

[108] ibid 146.

[109] Heather Harrison Dinniss, 'Cyber Warriors, Patriotic Hackers and the Laws of War' in D Saxon (ed.), *International Humanitarian Law and the Changing Technology of War* (Brill 2013) 251, 257. *Contra*, see V Padmanabhan, 'Cyber Warriors and the *Jus in Bello*' (2013) 89 *International Law Studies* 288, 295-296.

Secondly, it has been argued that hacker groups should be denied combatant status if they resort to techniques which make it impossible to distinguish between civilians and combatants.[110] These include, among others, the use of botnets, where civilian computers of unaware users are employed to launch a DDoS attack,[111] and IP spoofing, where the attacker masquerades his identity behind a civilian IP address.[112] The *rationale* behind this argument is that reliance on these techniques would place civilians at a risk of being targeted. However, it may be questioned whether this is a likely scenario.

To use a practical example, consider the ransomware attack launched by the CPB against the Belarusian railway network, and suppose that the CPB spoofed their IP address to make it look like the attack originated from the IP address of an unaware civilian user who lives somewhere near the border between Ukraine and Belarus. To conclude that such a civilian would be in danger of being counter-targeted is not persuasive since, as will be discussed *infra*,[113] the interplay between the principles of precaution and proportionality poses significant restraints, both legal and practical, on the targeting decisions of the Russian armed forces.

Rather, it is submitted that cyber attack techniques such as IP spoofing or the use of botnets should be considered lawful ruses of war, as they involve the use of deception and decoys.[114] Having said that, posing as civilians through cyber means is not permitted when it would violate the prohibition of perfidy. According to Art 37(1) of the AP I, it is prohibited to kill, injure or capture an adversary by resorting to perfidy, which comprises 'acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law

---

[110] Buchan (n 83) 752.
[111] CISA (n 12).
[112] Dinniss (n 12) 294. 'IP spoofing: How it Works and How to Prevent It', (*Kaspersky)* <https://www.kaspersky.com/resource-center/threats/ip-spoofing> accessed 3 May 2023.
[113] See Section Four.
[114] On the definition of ruses of war, see Art 37(2) of the AP I; Roscini (n 70) 215-216; see also *Tallinn Manual 2.0* (n 61) 495-496 for a non-exhaustive list of ruses of war in the cyber domain.

applicable in armed conflict, with intent to betray that confidence'.[115] This includes, *inter alia*, 'the feigning of civilian, non-combatant status.'[116]

Clearly, members of a hacker group that resort to perfidy through cyber means should not be entitled to combatant status. Note, however, that while is theoretically possible to envision cyber operations amounting to perfidy,[117] their practical occurrence seems unlikely,[118] if only because cyber operations rarely result in death or injury to *individuals*. Notably, damage or destruction of objects, which happens to be a more common occurrence of cyber operations, does not fall within the meaning of the prohibition.[119] In the case of the CPB, and based on the available information, they have not engaged in any cyber operation constituting perfidy.

2.6 *The Legal Status of the Cyber Partisans of Belarus*

The previous sections have concluded that the CPB do not satisfy the requirement of being under responsible command, they do not 'belong' to the government of Ukraine, and therefore are not entitled to POW status. At the same time, the CPB are both 'armed' and 'organized'. This raises the question as to the targetability of individuals belonging to an 'organized armed group' (OAG) who do not meet all the requirements for POW status.

In this regard, the most expansive approach to the issue has been adopted by the United States Department of Defence *Law of War Manual*, which treats the status of individuals 'belonging to a non-state armed group as a separate basis upon which a person is liable of attack, apart from whether

---

[115] AP I (n 39) art 37(1).
[116] ibid.
[117] For a discussion of the prohibition of perfidy in the cyber domain, see *Tallinn Manual 2.0* (n 61) 492-495.
[118] See, for instance, the example provided by the Cyber Law Toolkit and related analysis. 'State A discovers that commander X is a diabetic patient who uses a type of insulin pump that allows a healthcare provider to deliver the commander's insulin doses through a wireless communications system (i.e., a remote control). State A's cyber operatives hack into the pump's communications system, take over the remote control by using malware that authenticates itself as a legitimate third-party medical provider with insulin dosage permissions, and administer an overdose of insulin to commander X, which leads to X's death (**incident 2**). As a result, the operation accomplishes its main goal of killing the commander.' 'Scenario 15: Cyber Deception During Armed Conflict', Incident 2, (*Cyber Law Toolkit)* <https://cyberlaw.ccdcoe.org/wiki/Scenario_15:_Cyber_deception_during_armed_conflict#Perfidy_and_ruses_of_war> accessed 14 May 2023.
[119] *Tallinn Manual 2.0* (n 61) 495.

he or she has taken a direct part in hostilities.'[120] In other words, if a group is 'armed' and 'organized', its members can be targeted by virtue of their membership in the group, unless they are placed *hors de combat*.[121] Under this interpretation, members of the CPB would be at an increased risk of being targeted at all times by the Russian armed forces.[122]

A more restrictive view, which is the one that the present author adheres to, has been articulated by the *DPH Guidance,* which has argued that members of OAGs belonging to a Party to an IAC who do not fulfil the requirements for POW status should be considered combatants (that is, members of the armed forces) for the purposes of the conduct of hostilities. Accordingly, they can be targeted based on their 'continuous combat function' (CCF),[123] a concept that applies to individuals 'whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities.'[124]

Conversely, members of OAGs that do not belong to a Party to an IAC qualify as civilians, since doing otherwise would 'discard the dichotomy in all armed conflicts between *the armed forces of the*

---

[120] *US Law of War Manual* (n 67) [5.8.2.1].
[121] ibid.
[122] Note, however, that is unclear if Russia endorses this approach. The *Manual on International Humanitarian Law of the Armed Forces of the Russian Federation* does not provide any clarity on this issue, since it mentions the words 'organized armed groups' only once, in reference to the definition of NIAC. See Aleksei Romanovski, 'Manual on International Humanitarian Law of the Armed Forces of the Russian Federation - 2002' (2022) 99 ILS 772 at 775.
[123]See *DPH Guidance* (n 80) 33. In this regard, the notion of CCF has been introduced by the *DPH Guidance* to determine membership in an organized armed group in the context of a non-international armed conflict. According to the *DPH Guidance,* 'the decisive criterion for individual membership in an organized armed group is whether a person assumes a continuous function for the group involving his or her direct participation in hostilities' (pp. 33-36). The application of the concept of CCF in the context of an IAC is briefly mentioned by the *DPH Guidance* (p.25-26), which notes that 'Membership in irregular armed forces [...] belonging to a Party to the conflict can only be reliably determined on the basis of functional criteria, such as those applying to organized armed groups in non-international armed conflict';
See also Sabrina Henry, 'Exploring the "Continuous Combat Function" Concept in Armed Conflicts: Time for an Extended Application?' (2018) 100 International Review of the Red Cross 267, 276, where the author notes that 'In its Interpetive Guidance, the ICRC suggests using the concept of CCF [...] to determine individual membership in an organized armed group in IAC'; Michael Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) (1) Harvard National Security Journal 21-22, noting that 'The continuous combat function idea initially surfaced in the context of non-international armed conflict. […] Over the course of the meetings, this criterion slowly bled into international armed conflicts; its evolution is reflected in the fact that the Interpretive Guidance discusses the criterion with regard to international armed conflict only in passing and entirely by reference to its application during non-international armed conflict'.
For a critique of the concept, see Schmitt (n 123); William Boothby, 'And For Such Time As: The Time Dimension to Direct Participation in Hostilities' (2010) 42 New York University Journal of International Law and Politics 741, 743; Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance' (2010) 42 New York University Journal of International Law and Politics 641, 655-657.'
[124] *DPH Guidance* (n 80) 34.

parties to the conflict and the *civilian population*.'[125] However, members of such a group can still be regarded as parties to a separate NIAC 'provided that the violence reaches the adequate threshold' of intensity,[126] namely that of 'protracted armed violence'.[127] In such a case, they can be targeted according to their CCF.[128]

Where do the CPB fall within these categorizations? As already stated, the CPB are members of an OAG which does not belong to a Party to an IAC. Moreover, they cannot be considered as parties to a separate NIAC: while theoretically possible, it is very unlikely that cyber operations alone can reach the required threshold of intensity.[129] The cyber operations launched by the CPB make no exception to this statement: while these cyber operations, as it will be argued *infra*,[130] affect the military capacity of Russia and would qualify as DPH, they do not reach the threshold of 'protracted armed violence' necessary for the existence of a NIAC.

Therefore, it is submitted that members of the CPB qualify as civilians who, if captured, would not be considered POWs, but would fall within the scope of the GCIV. Moreover, they are protected from attack unless and for such time they take a direct part in hostilities.

3 The Notion of Direct Participation in Hostilities in the Russia-Ukraine Cyber Conflict

The previous section has concluded that both the IT Army and the CPB qualify as civilians, demonstrating how, in practice, it is very unlikely that a hacker group would satisfy the requirements of combatancy, even if an adaptive interpretation is adopted. The case of the CPB is especially

[125] *DPH Guidance* (n 80) 23-24. Italics added.
[126] ibid. The *DPH* Guidance further notes that 'organized armed violence failing to qualify as an international or a non-international armed conflict remains an issue of law enforcement.'
[127] *Prosecutor v Dusko Tadic (*Decision on the Defence Motion on Interlocutory Appeal on Jurisdiction) IT-94-1 (2 October 1995) [70].
[128] *DPH Guidance* (n 80) 71.
[129] *Tallinn Manual 1.0* (n 61) 85, noting that 'Given the requisite threshold of violence [...] cyber operations in and of themselves will only in exceptional cases amount to a non-international armed conflict.'
[130] See Section 3.2.2.

illustrative of the reduced relevance of combatant status in the cyber domain, as the CPB have disclosed information about their goals and internal structure differently from the secrecy in which hacker groups normally operate. Given that both the CPB and the members of the IT Army are civilians, they are protected from attack unless and for such time as they take a direct part in hostilities.

Accordingly, the following sections will discuss the extent to which their cyber operations amount to acts of DPH, alongside individual civilians who have supported Ukraine through the use of online apps and social media.

3.1 *The Cyber Domain and the Concept of Direct Participation in Hostilities*

According to the ICRC, the notion of DPH comprises three requirements which must be cumulatively satisfied: threshold of harm, direct causation and belligerent nexus.[131] *Threshold of harm* is satisfied when an act causes death or injury to civilians, damage or destruction to objects, or a combination thereof.[132] Alternatively, an act may cause what the ICRC calls 'military harm', by 'adversely affecting the military capacity of one party to the conflict.'[133] Note that these conditions do not have to happen simultaneously, as either will suffice.

In the cyber domain, the first limb of the test is very unlikely to be satisfied since cyber operations do not generally result in physical violence. Similarly to what has been suggested in relation to the notion of 'attack' under Art 49 of the AP I, it can be questioned whether the threshold of harm requirement should be adapted to include cyber operations that result in severe adverse consequences of a non-violent nature against the civilian population and civilian objects.[134] While this approach allows IHL to adapt itself to the disruptive potential of cyber technologies, it must be cautioned that

[131] *DPH Guidance* (n 80) 46.
[132] ibid..
[133] ibid 47.
[134] In this regard, see *Tallinn Manual 2.0* (n 61) 429: 'The act…must have the intended or actual effect of negatively affecting the adversary's military operations or capabilities, or inflicting death, physical harm, or material destruction on persons or objects protected against direct attack (threshold of harm)'; Ido Kilovaty, 'ICRC, NATO and the US – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law' (2016) 15(1) Duke Law and Technology Review 1, 20-29; Roscini (n 70) 206; Nils Melzer, *Cyberwarfare and International Law* (*UNIDIR,* 2011) 29.

it would inevitably expand the scope of application of the notion of DPH, increasing the number of potential cyber direct participants who can be targeted.

The second criterion, *direct causation*, requires the harm to occur in a single causal step,[135] except for acts which form an integrated part of a coordinated military operation during which such harm is caused.[136] The requirement appears to be too restrictive in the cyber domain, considering that cyber operations often result in reverberating or 'second order' effects. As opposed to 'first order' effects, which are the 'immediate [...] consequences of an attack'[137], second order effects are the 'delayed and displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms.'[138]

To better illustrate this point, consider the ransomware attack launched by the CPB against the Belarusian railways. The ransomware produced first order, or direct effects, when the malware successfully infected the targeted systems, so that they could not perform their intended task. Any effect resulting from disrupting the functionality of Belarusian railway's servers is therefore an indirect effect of the ransomware, including the stoppage of trains and the slowing down of the Russian supply chain and movement of troops. As such, interpreting direct causation as synonymous with direct effects would exclude a vast amount of cyber operations from ever satisfying the requirement.[139]

It is submitted that a better approach is to consider the direct causation requirement satisfied for any consequential damage that is connected to the original act by an uninterrupted causal chain of events.[140] In other words, what matters is that the harmful effects of a cyber-operation could not have

---

[135] *Tallinn Manual 2.0* (n 61) 51.
[136] ibid.
[137] Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at II-35 (2007).
[138] ibid.
[139] For similar concerns, see D Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) *Journal of Conflict and Security Law* 279, 288.
[140] That does not mean *all* delayed effect would be included in the direct causation requirement, but only those that occur within such an uninterrupted causal chain. As noted by the *DPH Guidance*, causal proximity must be kept distinct from geographical and temporal proximity. See *DPH Guidance* (n 80) 66.

occurred 'but for' the cyber-operation itself.[141] Finally, the belligerent nexus criterion requires that the act must be specifically designed to cause the required threshold of harm in support of a party to the conflict and to the detriment of another.[142] The *rationale* of the requirement is to exclude cyber operations motivated by criminal purposes or that satisfy the two requirements of threshold of harm and direct causation but do so in an incidental manner. In the cyber domain, the assessment of the requirement can be hindered by the secrecy that surrounds cyber operations that would otherwise constitute an act of DPH. As it will be discussed *infra*, that has not been the case in the context of the Russia-Ukraine cyber conflict.

Finally, individuals who commit DPH can only be targeted 'for such time as' they take a direct part in hostilities. This timeframe includes the preparation of the act, the deployment phase, and the return from the act.[143] Furthermore, the *DPH Guidance* clarifies that 'civilians lose and regain protection against direct attack in parallel with the intervals of their engagement in direct participation in hostilities'.[144] This approach has been criticized since it results in a 'revolving door of protection' whereby civilians are protected from attack between each act constituting DPH, making targeting decisions all the more difficult for belligerents.[145]

In the cyber domain, an act of direct participation can be instantaneous, resulting in a window of targetability that is practically non-existent.[146] Even considering that the temporal loss of protection within each act of direct participation extends to the preparation of the act, many preparatory acts can only be assessed *ex-post*, rather than deduced *ex-ante*. Considering again the ransomware launched by the CPB, such a cyber operation involves preparatory acts like accessing the target network to probe it for possible vulnerabilities which would make the deployment of the ransomware more

[141] On the 'but for' approach to the direct causation test, see Schmitt (n 123) at 29.
[142] *DPH Guidance* (n 80) 58.
[143] ibid 65.
[144] ibid 69.
[145] *US Law of War Manual* (n 67) at 276: 'Persons who take a direct part in hostilities, however, do not benefit from a "revolving door" of protection.' See also Boothby (n 123) 753-759; Watkin (n 123) 686-690; Schmitt (n 123) 37-38.
[146] D Wallace and S Reeves, 'Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines' (2021) 12 Harvard National Security Law Journal 164, 186; *DPH Guidance* (n 80) 53.

effective. However, the mere intrusion within a network is not *per se* conclusive that an act of DPH will be committed, unless there is additional information that the CPB intend to do so and the intrusion in the network is, in fact, the first step of committing an act of DPH.

A separate issue arises when an individual performs multiple acts of cyber-participation over a certain timespan, a scenario for which the experts involved in the drafting of the *Tallinn Manual* were divided, with the majority endorsing the ICRC's approach that each act of direct participation should count as an isolated act,[147] and the minority arguing that the temporal window of targetability should cover the whole time in which an individual has engaged in cyber operations amounting to DPH.[148] In this regard, it is submitted that the latter approach is preferrable, as it gives belligerents a reasonable window of opportunity to target a cyber direct participant.[149]

3.2 *The Notion of Direct Participation in Hostilities in the Russia-Ukraine Cyber Conflict*

The article will now focus on the applicability of the notion of DPH to specific cyber-operations which took place during the Russia-Ukraine cyber conflict, namely those conducted by the IT Army, the ransomware attack launched by the CPB in late February 2022, and the sharing of military intelligence by civilians.

3.2.1 Cyber Operations Launched by the IT Army of Ukraine Against Russian Targets

It is submitted that the DDoS operations launched by the IT Army do not constitute acts of direct participation, including several attacks on Russian private entities, Russian governmental websites, as well against the Wagner Group. To be considered as DPH, these cyber operations need to satisfy the threshold of harm requirement by causing death or injury to civilians, or damage or destruction to objects or, alternatively, they must adversely affect the military capacity of Russia.

---

[147] *Tallinn Manual 2.0* (n 61) 432; *DPH Guidance* (n 80) 44-45, 70-71.
[148] ibid.*;* Schmitt (n 58) 13. See also Y. Dinstein (n32) 202, suggesting that the temporal loss of protection should extend 'as far as 'upstream' and 'downstream' as a causal link exists'.
[149] Wallace and Reeves (n 146) 193.

From the information available, the impact of these cyber operations has been varied. At the lowest end of the spectrum are website defacements, such as the one against the Russian space agency RosKosmos, consisting in the posting of messaging honoring the Ukrainian Constitution Day.[150] Such a cyber operation does not qualify as an act of DPH as it did not cause any death or injury to individuals, or damage or destruction to objects, nor did it affect the military capacity of Russia. A similar conclusion can be drawn in relation to the waves of DDoS attacks launched by the IT Army against civilian targets like banks, online pharmacies, and other companies, which created a moderate inconvenience but did not cause any violence to individuals or objects.[151]

Finally, the IT Army also reportedly hacked the website of the Wagner Group, a Russian PMC with close ties to the Kremlin, claiming to have stolen personal data of members of the group.[152] However, even considering that the Wagner Group as an armed group belonging to Russia through a *de facto* relationship,[153] the stealing of personal data does not affect Russia's military capacity, unless it can be proved that several members of the Wagner group have been demoralized as a result of the hack, and their military operations have been slowed down or compromised as a result. Though it is not possible to estimate whether the operation has adversely affected the military capacity of Russia,[154] this does not seem to be the case.

---

[150] 'The IT Army attacked more than 800 Russian websites in two weeks – Ministry of Digital Transformation' (*Ukrinform*, 11 July 2022) <https://www.ukrinform.net/rubric-ato/3526518-it-army-attacks-over-800-russian-websites-in-two-weeks-ministry-of-digital-transformation.html>.

[151] See, for instance, for instance, the hacking of the Russian Taxi company 'Yandex'. E Roth, 'Hackers Caused a Massive Traffic Jam in Moscow Using a Ride-Hailing App' (*The Verge,* 3 September 2022) <https://www.theverge.com/2022/9/3/23335694/hackers-traffic-jam-russia-moscow-ride-hailing-app-yandex-taxi>.

[152] Lorenzo Franceschi-Bicchierai, 'Pro-Ukraine Hacktivists Claim to Have Hacked Notorious Russian Mercenary Group' (*VICE,* 20 September 2022) <https://www.vice.com/en/article/4ax459/pro-ukraine-hacktivists-claim-to-have-hacked-notorious-russian-mercenary-group>.

[153]See generally Lindsay Cameron and Vincent Chetail, *Privatizing War: Private Military and Security Companies Under International Law* (Cambridge University Press 2013) 204-223. See also Michael Rizzotti, 'Russian Mercenaries, State Responsibility, and Conflict in Syria: Examining the Wagner Group Under International Law' (2020) 37(3) Wisconsin International Law Journal 569; J Maddocks, 'Russia, the Wagner Group, and the Issue of Attribution' (*Articles of War*, 28 April 2021) <https://lieber.westpoint.edu/russia-wagner-group-attribution/>.

[154] For the opposite argument, see Biggerstaff (n 56).

A similar conclusion can be drawn with regards to the hacking of the Russian central bank, which revealed financial transaction of the Ministry of Defence, as well as card and phone numbers of members of Russian military personnel.[155]

In conclusion, none of the above-mentioned cyber operations qualify as an act of DPH because they do not reach the required threshold of harm. As such, members of the IT Army qualify as civilians who are protected from attack since they are engaging in cyber operations not amounting to DPH.

3.2.2 Ransomware Attack Against the Railway Network of Belarus

It is submitted that the ransomware attack launched by the CPB qualifies as an act of DPH. In relation to the threshold of harm requirement, the ransomware did not cause any physical violence. Nonetheless, it was directed against a military objective,[156] the railway network of Belarus, which has been used by Russia to move its troops from its western border into northern Ukraine. Moreover, on 29 February 2022 the spokesperson of the CPB claimed that, due to the ransomware, the Belarusian Railway network had to rely on manual control, since its train traffic controller system had been disabled. As a result, the lines between Minsk and Orsha, near the western Russian border, were paralyzed.[157]

In this regard, the ICRC recognizes that 'disturbing deployment, logistics and communication' can adversely affect the military capacity of a party to the conflict.[158] Considering the reliance by the

---

[155] Akshaya Asokan, 'IT Army of Ukraine Targets Russian Banks', (*BankInfo Security*) <https://www.bankinfosecurity.com/ukrainian-army-targets-russian-banks-a-20443> accessed 12 May 2023.

[156] Military objectives are defined as 'objects that, by their nature, location, purpose, or use, make an effective contribution to military action, and whose total or partial destruction, capture, or neutralization offers a definite military advantage'. See AP I (n 39) Art. 52. On railroads qualifying as military objectives, see Dinstein (n 32) 129, 143; Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013) 120 ('HPCR Manual').

[157] Belarusian Cyber-Partisans, 'Belarusian Railway Has Been Switched to Manual Mode of Operation' (*Twitter,* 27 February 2022) <https://twitter.com/cpartisans/status/1497969171812036615> accessed 12 May 2023; Adam Smith, 'Hackers Attack Train Network to Stop Putin Moving Troups from Russia to Ukraine' (*The Independent,* 28 February 2022) <https://www.independent.co.uk/tech/hackers-attack-train-putin-troops-russia-ukraine-b2024907.html.> accessed 12 May 2023.

[158] *DPH Guidance* (n 80) 48.

Russian army on railway networks, it can be argued that the ransomware attack adversely affected its military capacity. As such, the requirement of threshold of harm is satisfied.

As for direct causation, the approach of the ICRC is again too restrictive because the military harm caused by the ransomware took place in distinct causal steps. Nevertheless, under the more expansive interpretation provided above,[159] the act satisfies the requirement of direct causation since the harm was brought about through an uninterrupted causal chain of events that started when the ransomware against the Belarusian railway network was deployed.

Finally, the ransomware was specifically designed to harm Russia and support Ukraine, as publicly stated by the CPB's spokesperson,[160] and therefore satisfies the requirement of a belligerent nexus. Consequently, the ransomware against the Belarusian railway could qualify as an act of DPH. In relation to the temporal loss of protection from attack, the temporal window of targetability that began when they deployed the ransomware against the Belarusian railway network has now elapsed, and there is no available information as to whether they are planning similar operations in the near future.

3.2.3 Sharing of Military Intelligence

Since Russia invaded Ukraine, the sharing of military intelligence by civilians has been constant[161] Intelligence sharing has been conducted through the use of Telegram and dedicated apps. For instance, the Ukrainian government has encouraged Ukrainian civilians to geolocate the presence of Russian troops, military equipment, or weaponry through the eVorog chatbot within Telegram,[162] to signal the presence of cruise missiles and kamikaze drones by downloading the app ePPO,[163] and to share this information with the armed forces of Ukraine. In other instances, military intelligence sharing has

[159] See *supra* Section 3.1.
[160] *Belarusian Cyber-Partisans* (n 158).
[161] Harwell (n 25)
[162] ibid.
[163] Sabbagh (n 26).

been independently conducted by hacker collectives such as the CBP, who have been collaborating to this end with the Kastus Kalinowski regiment since the Russian invasion of Ukraine.[164]

In this regard, it is submitted that all of the above examples constitute acts of DPH.[165] To begin with, these operations affect the military capacity of Russia because the information, once passed on to the armed forces of Ukraine, have led to the targeting of Russian soldiers, military equipment, or weaponry. For instance, in September 2022, the Ukrainian army was able to destroy Russian military vehicles that were stored in a warehouse in Kherson one day after being alerted by local residents through EVorog.[166] On another occasion, a Kalibr cruise missile was shut down immediately after being reported by Ukrainian civilians using the ePPO application.[167]

Note, moreover, that the destruction of Russian military objectives by the Ukrainian armed forces from the sharing of military intelligence is not necessary to satisfy the threshold of harm requirement. What suffices, instead, is the *likelihood* that the harm occurs, not its actual materialization.[168] In relation to the direct causation requirement, intelligence sharing operations cause the harm in different causal steps. Like what has been said in relation to the CPB ransomware attack, such harm is the result of an uninterrupted causal sequences that begins when the information is passed to the armed forces of Ukraine and ends when the target is successfully attacked. That said, even without resorting to a more expansive interpretation of direct causation, it can be submitted that the requirement would still be satisfied, as all of the above examples constitute 'an integral part of a concrete and tactical operation that directly causes such harm.'[169]

---

[164] Gostoli (n 90).
[165] See generally *Tallinn Manual 2.0* (n 61) 430: 'Other unambiguous examples include gathering information on enemy operations by cyber means and passing it to one's own State's armed forces'; *DPH Guidance* (n 80) 55.
[166] 'How a Chatbot Has Turned Ukrainian Civilians Into Digital Resistance Fighters' (*The Economist,* 22 February 2023) <https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters> accessed 1 May 2023.
[167] 'Ingenious Mobile App Helps Down First Russian Missile in Ukraine', (*Ukrinform,* 26 October 2022) <https://www.ukrinform.net/rubric-ato/3601566-ingenious-mobile-app-helps-down-first-russian-missile-in-ukraine.html> accessed 1 May 2023.
[168] *DPH Guidance* (n 80) 47.
[169] Michael Schmitt and Casey Biggerstaff, 'Ukraine Symposium – Are Civilians Reporting with Cell Phones Directly Participating in Hostilities?' (*Articles of War,* 2 November 2022) <https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/> accessed 3 May 2023.

Finally, these operations also satisfy the requirement of belligerent nexus, as their objective purpose is to support Ukraine to the detriment of Russia. In conclusion, the sharing of military information by the CPB and by individual civilians using eVorog or ePPO qualifies as an act of DPH for which they lose their protection from attack for the duration of their direct participation. With regards to this point, the CPB have been consistently sharing information with the KKR as part of their cooperative relationship. Likewise, it can be assumed that individual civilians might have used EVorog and EPPO in multiple instances. Both scenarios may involve repeated acts of DPH and, depending on the length of time between each act of participation, the targetability window may vary.

Consider, for instance, the case of a civilian that has sent the geolocation of Russian troops using eVorog on one day, stops for one month, then resumes sharing military intelligence. In this case, the loss of protection from attack only lasts for each repeated act of direct participation, making the window of targetability extremely narrow. Conversely, if the same individual is giving valuable information to the Ukrainian armed forces every day for the same timeframe, he would be targetable for the whole time he engages in DPH until he 'unambiguously opt[s] out of hostilities through extended non-participation or an affirmative act of withdrawal'.[170] In this case, citizens can withdraw from hostilities and participation by uninstalling the ePPO application or avoiding using the eVorog chatbot altogether.

This does not mean, however, that the targeting of such individuals would be practically feasible, since it would depend on identifying the civilian direct participant from an IP address, pinpointing the exact location, and then planning an attack, which would have to comply with the principles of proportionality and precaution in attack under Additional Protocol I and Customary IHL. By the time the necessary information has been gathered, the targetability window might have already elapsed.

---

[170] Michael Schmitt, 'Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees' (2005) 5 Chicago Journal of International Law 511, 534; Kenneth Watkin, 'Humans in the Cross-Hairs: Targeting and Assassination in Contemporary Armed Conflict' in David Wippman and Matthew Evangelista (eds.), *New Wars, New Laws: Applying Laws of War in 21st Century Conflicts* (Brill 2005) 137-167.

4 The Targeting of Cyber Direct Participants in the Russo-Ukraine Cyber Conflict

Unlike members of the IT Army, members of the CPB and individual civilians that commit an act of DPH through cyber means forfeit their protection from attack for such time as their direct participation endures. Therefore, they can be lawfully targeted via kinetic means and injured or killed by the Russian armed forces. Considering the relative ease with which it is possible to use the eVorog chatbot or the ePPO application to transmit military intelligence to the armed forces of Ukraine, it can be submitted that civilian cyber direct participation in hostilities will continue to take place in the Russia-Ukraine armed conflict. It can further be submitted that cyber direct participation in hostilities will be a constant in future armed conflicts where cyber technologies will play a significant role.

In light of the ever-increasing number of cyber direct participants, it appears evident how cyber warfare may increase the instances in which lethal force can be lawfully deployed by belligerents not just *vis-à-vis* cyber participants, but also against any object that qualifies as a military objective by enabling acts of direct participation through cyber means, such as telecoms infrastructures.[171] But as the *quantum* of violence in the battlefield is enhanced by cyber technologies, so is the potential for greater human suffering. Thus, this calls into question the extent of which IHL can effectively constrain the recourse to lethal force and pursue its core aim of protecting the civilian population in times of armed conflict.

As highlighted in Section One, this objective is achieved at the normative level by balancing military necessity and humanitarian consideration through the principle of distinction, which protects civilians

[171] Vera Bergengruen, 'The Battle for Control Over Ukraine's Internet', (*Time,* 18 October 2022) <https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/> accessed 3 May 2023; Thomas Brewster, 'Ukraine Engineers Battle to Keep the Internet Running While Russian Bombs Fall Around Them', (*Forbes,* 22 March 2022) <https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/?sh=3188cbf25a4c> accessed 3 May 2023.

from direct attack. Conversely, IHL does not prohibit the incidental killing or harming of civilians, since it is unavoidable that an attack against a lawful target may result in civilian death and injury, or in destruction of civilian objects. This does not mean, however, that belligerents have *carte blanche* in the conduct of their military operations. On the contrary, IHL attempts to minimize the amount of civilian death and destruction through the principles of proportionality and precaution in attack.

With regards to the principle of proportionality, Art 51(5)(b) of the AP I prohibits attacks which are expected to cause an amount of 'collateral damage', incidental loss of life or injury to civilians, damage or destruction to civilian objects, or a combination thereof, which would be excessive in relation to the military advantage anticipated from an attack.[172] In relation to the principle of precautions in attack, Art 57 of the AP I provides several obligations incumbent on those who decide or plan an attack, primarily aimed at avoiding or minimizing collateral damage.

4.1 *The Principles of Proportionality and Precaution in the Russia-Ukraine Cyber Conflict*

To illustrate how the principles of proportionality and precaution operate in practice and the extent to which they can constrain the attacker, the following sections will examine the targeting of a direct participant whop has been transmitting information to the armed forces of Ukraine using the eVorog chatbot.

4.1.1 Precautions in Attack

To begin with, those who plan or decide on an attack are under the obligation to do everything feasible to verify that the individual is a lawful target and not a civilian.[173] To this end, Art 57(2)(b) of the AP I provides that an attack shall be suspended or cancelled if it 'becomes apparent that the objective is not a military one.'[174]

[172] AP I (n 39) art 51(5)(b); *Customary International Humanitarian Law* (n 28) Rule 14.
[173] AP I (n 39) art 57(2)(a)(i); *Customary International Humanitarian Law* (n 28) Rule 15.
[174] AP I (n 39) art 57(2)(b).

The obligation to do 'everything feasible' which underpins Art 57 of the AP I should be understood as a standard of due diligence which requires military planners do to that which is practically possible considering 'all the circumstances ruling at the time including humanitarian and military considerations',[175] such as the quantity and quality of resources and technology available to the attacker as well as the risk to the attacking forces. Thus, it does not amount to an absolute requirement of doing everything possible.[176]

As far as the obligation to verify is concerned, at a minimum it requires a military commander to 'set up an effective intelligence gathering system to collect and evaluate information concerning potential targets' and employ 'available technical means to properly identify targets during operations.[177] In the cyber domain, a military commander should employ specific verification techniques, such as 'network mapping' and 'footprinting', the purpose of which is to identify 'the ownership and geographical locations of the targets and related infrastructure' where cyber operations will be conducted or cyber effects are expected to occur, and 'to identify the people and entities that could be affected by proposed operations'.[178]

In the example provided above, the Russian armed forces must identify the direct participant from an IP address, locate the physical address, and then ensure that the individual is still within the temporal window of targetability during which they are not protected from direct attack. This would require determining if the individual has been transmitting military intelligence or an occasional or continuous basis. In the former case, the individual would be protected from attack right after the act of direct participation would end, resulting in a very narrow targetability window. In the latter case, the temporal loss of protection from attack would last until he decides to unambiguously opt out of

---

[175] United Kingdom, *The Manual of the Law of Armed Conflict* (Ministry of Defence, 1 July 2004) [5.32], footnote 191; United Nations, *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (Amended on 21 December 2001)*, 10 October 1980, 1342 UNTS 137, Protocol II at 192; Frederic De Mulinen, *Handbook on the Law of War for Armed Forces* (*ICRC,* 1987) [365].
[176] *US Law of War Manual* (n 67) [5.2.3.2].
[177]See ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (2000) [29].
[178] 'US Presidential Policy Directive/PPD-20' (20 October 2012) 7. See Roscini (n70) 235.

hostilities. In practice, this part of the verification process should ascertain how many times the individual has submitted information through eVorog or ePPO, and whether they have signalled their intention to do so in the future by posting on social media or in private communications.

In cases where the verification process results in doubt as to the status of a person, the presumption of civilian status introduced by Art 50(1) of the AP I would apply.[179] Clearly, this would mean that the individual in question cannot be attacked and, if the attack is underway, the attack must be cancelled or suspended.[180]

A different legal issue arises when the identity of the direct participant has been ascertained but doubt still persists as to whether the individual has regained protection from attack. This situation falls outside the scope of application of Art 50(1) of the AP I, since the direct participant is, by definition, a civilian.[181] In a similar scenario, the attacker must 'review all of the relevant information and act reasonably in the circumstances when deciding whether to conduct the attack'.[182]

Once an individual has been verified to be a lawful target of attack, the principle of proportionality comes into play, both as part of the prohibition on indiscriminate attacks, and as a component of the rules on precaution related to the planning and execution of the attack.[183] In accordance with Art 57(2)(a)(ii) of the AP I, Russian military commanders are under an obligation to do everything feasible, in the choice of methods and means of warfare, to avoid or in any event minimize collateral damage.[184] This provision shares a similar logic with Art 57(3) of the AP I, which applies to situations where a choice is possible between different military objectives, each one resulting in the same degree

[179] AP I (n 39) art 50(1). This provision also reflects Customary IHL. See *Customary International Humanitarian Law* (n28) Rule 6.
[180] AP I (n 39) art. 57(2)(b).
[181] Michael Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 New York Journal of International Law and Policy 697, 736-737. *Contra*, see *DPH Guidance* (n 80) at 75-76. The issue of whether a presumption against direct participation exists has been discussed in the Tallinn Manual. See *Tallinn Manual 2.0* (n 61) 432.
[182] ibid 43; Richard Guelff, Adam Roberts, *Documents on the Laws of War* (Oxford University Press 1998); Spanish Declaration E, 509.
[183] Sandoz (n 53) 683, [2204]-[2205].
[184] AP I (n 39) art 57(2)(a)(ii). See also Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nihjoff 2009) 168, noting that 'In other words, there is a requirement to minimize collateral damage and not merely to cause no more than proportionate damage.'

of military advantage. In this case, those who plan or decide upon an attack must select the military objective that, when attacked, would result in the least amount of collateral damage.[185]

While the potential of both rules in protecting the civilian population against the adverse effects of kinetic attacks taken in response to an act of DPH in cyberspace may seem evident at first glance, their interpretation must always factor military necessity considerations. In relation to Art 57(2)(a)(ii) of the AP I, there is no obligation for attacking forces to choose a method of attack which completely avoids or minimizes collateral damage. Armed forces can select another method of attack which is expected to cause more collateral damage, but would result in a greater amount of military advantage.[186]

This, in turn, reduces the applicability of Art 57(3) of the AP I, as it is hard to fathom a scenario where choosing to target a military objective with cyber means would result in a military advantage similar to the targeting of a different military objective with kinetic weapons.[187] In practical terms, if Russian military commanders can choose between targeting a civilian cyber participant with kinetic force or hacking their device to prevent the sharing military intelligence, they would be permitted to opt for the former because it will result in more of a military advantage compared to the latter. [188]

4.1.2 The Proportionality Equation: Comparing Anticipated Military Advantage with Expected Collateral Damage

In accordance with Art 57(2)(a)(iii) of the AP I, military commanders must compare the expected collateral damage from targeting the direct participant with the anticipated military advantage gained from the attack and, if the latter exceeds the former, they must cancel the attack.[189] Similarly, Art 57(2)(b) of the AP I requires commanders to do everything feasible to cancel or suspend an attack

[185] AP I (n 39) art 57(3)2.
[186] Michael Schmitt, 'International Humanitarian Law and the Conduct of Cyber Hostilities: *Quo Vadis*?' (2022) 13 JIHLS 189, 215-216. See also Seth Lazar, 'Necessity in Self-Defense and War' (2012) 40 Philosophy and Public Affairs 3, 23.
[187] For instance, attacking a power grid with kinetic weapons results in more military advantage than disrupting the functionality of the operating network of the same power grid with a cyber attack. Therefore, the attacker can opt for the former method of attack, assuming that this attack is not expected to result in excessive collateral damage.
[188] Henderson (n 185) 189-190.
[189] AP I (n 39) art 57(2)(a)(iii).

which is underway if it becomes apparent that it would violate the principle of proportionality.[190] Failure to comply with either obligations would result in launching an attack which would be considered disproportionate within the meaning of Art 51(5)(b) of the AP I.

At the core of both provisions is the proportionality equation, the first element of which is the quantification of the *concrete* and *direct* military advantage anticipated from the attack. The term 'concrete' has been interpreted as requiring the existence of a tangible or measurable effect. In contrast, 'direct' relates to the chain of causation between the attack and the military advantage, which must happen 'without intervening condition of agency' and to the exclusion of indirect and purely speculative military advantages.[191] Furthermore, the *concrete* and *direct* military advantage from the attack must be assessed 'as a whole', rather than from isolated and specific parts of the attack. [192]

In the situation described above, it can be questioned what the 'concrete and directed military advantage' anticipated from targeting a cyber participant who is geolocating Russian troops is. It should be pointed out that the concept of military advantage also includes force protection, the minimization by the attacking party of the risk to its own soldiers' safety.[193] Since sharing the location of Russian troops enables the Ukrainian Armed Forces to attack them, targeting a direct participant would provide both a concrete and direct military advantage by preventing Russian troops from being attacked. Evidently, the *quantum* of military advantage always depends on the circumstances of the case: the more an individual has shared military intelligence on eVorog,[194] the higher the amount of anticipated military advantage.

---

[190] AP I (n 39) art 57(2)(b).
[191] A Rogers, *Law on the Battlefield* (Manchester University Press 1996) 99.
[192] Andreas Laursen, 'NATO, the War Over Kosovo, and the ICTY Investigation' (2002) 17 American University International Law Review 765, 795; Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press 2004) 102; Henderson (n 185) 200; Roscini (n 70) 226; Dinstein (n 32) 134.
[193] Robin Geiss, 'The Principle of Proportionality: Force Protection as Military Advantage' (2012) 45(1) *Israel Law Review* 71, 78.
[194] As of 6 August 2022, eVorog has received close to 350,000 alerts. It is safe to assume that at least some of these alerts may have come from the same source, that is, the same direct participant. See 'Enemy-Spotting Chatbot in Ukraine Boasts Over 344,000 Reports' (*Ukrinform,* 6 August 2022) <https://www.ukrinform.net/rubric-ato/3544619-enemyspotting-chatbot-in-ukraine-boasts-over-344000-reports.html> accessed 13 May 2023.

Once Russian commanders have determined the *quantum* of military advantage anticipated from the attack, they must quantify the expected collateral damage. In practice, the amount of expected collateral damage may vary depending on the location of the direct participant. If the individual is in a densely populated neighbourhood, there is a higher risk of causing collateral damage as opposed to if they were in rural area. In any case, even an *extensive* amount of collateral damage would not be immediately deemed *excessive*, as the concept is relative to the anticipated military advantage gained from the attack: the higher the anticipated military advantage, the higher the amount of collateral damage that would be permitted before the obligations of refraining from launching or suspending an attack would apply.[195]

After the expected collateral damage and the anticipated military advantage have been quantified, they must be measured against each other and, if the former is *excessive* to the latter, the attack must be cancelled or suspended. This comparison requires an inherently subjective assessment that involves two 'incommensurable' values[196] and can yield different results, not only among military planners within the same armed forces, but across military cultures as well.[197] As a result, opposing parties are likely to evaluate the components of the proportionality equation in different ways.[198] In other words, it is possible that the attacker would assign a greater weight to the anticipated military advantage than the expected collateral damage, while the defender's assessment of the proportionality equation may lead to the opposite conclusion.[199]

Therefore, whether a certain amount of collateral damage would be deemed *excessive* varies depending on the *quantum* of military advantage anticipated from targeting a direct participant in the circumstances of the case. Targeting a direct participant who has occasionally shared military

---

[195] Amichai Cohen and David Zlotogorski, *Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures* (Oxford University Press 2021) 100; HPRC Manual (n 156) 92.
[196] Robert Sloane, 'Puzzles of Proportion and the "Reasonable Military Commander": Reflections on the Law, Ethics, and Geopolitics of Proportionality' (2015) 6 Harvard Security Law Journal 299, 321.
[197] International Criminal Tribunal for the Former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic Of Yugoslavia* (8 June 2000) 50.
[198] Dinstein (n 32) 158.
[199] Dieter Fleck, 'Strategic Bombing and the Definition of Military Objectives' (1997) 27 Israel Yearbook on Human Rights 48.

intelligence would result in a modest military advantage, as opposed to an individual who has been constantly submitting pictures and videos of Russian troops and equipment on eVorog. In the former situation, it is then logical to assume that only a low amount of expected collateral damage would not be considered as *excessive*. Conversely, a greater amount of expected collateral damage would be permitted in the latter case.

5 Conclusion

The present article has discussed the legal status and the targeting of individuals who have engaged in cyber operations to support Ukraine in the Russia-Ukraine armed conflict. Considering that resulting legal picture is one of legal uncertainty, some identifiable key points are warranted.

To begin with, reliance on cyber technologies results, predictably, in an increase in the civilianization of armed conflict. Among the various actors that have contributed to the cyber conflict to support Ukraine, the qualification of members of the IT Army is the least problematic: due to the lack of accurate information available on their structure and hierarchy, it is submitted that they qualify as civilians who have, so far, engaged in cyber operations below the threshold of DPH. Conversely, the case of the CPB demonstrates how the law of combatancy can be difficult to apply in the cyber domain. This is partly due to the fact that the requirements of distinction have a diminished relevance in the cyber domain, and partly because requirements such as those of organization and responsible command are unlikely to be satisfied by hacker groups, who for the most part conduct their operations in secrecy. As such, this Article has argued that members of the CPB qualify as civilians who do not enjoy POW status in the (rare) event of capture but would be protected by the Fourth Geneva Convention.

In relation to targeting, this Article aligns with the approach of the *DPH Guidance*: members of the CPB can be attacked ‘for such time as’ they directly participate in hostilities, even though the extent to which they risk being targeted is hard to estimate, especially considering the issues in evaluating

the temporal loss of protection from attack. Note, however, that if Russia were to align to the position of the United States' *Law of War Manual*, members of the CPB could be targetable at all times. [200] This would place them at a considerable risk for their safety.

Secondly, software such as eVorog and ePPO enable an ever-growing number of civilians to commit repeated acts of DPH with relative ease. The key question is if this could lead to an increase in the amount of violence that can be lawfully deployed on the battlefield. On the one hand, compliance with the rules on targeting places significant restraints on Russian armed forces, considering that target verification appears particularly difficult in the cyber domain. Moreover, the anticipated military advantage gained from targeting a single direct participant may be, depending on the circumstances, so modest as to only permit attacks expected to cause a low amount of collateral damage, or no collateral damage at all. Taken together, these two factors should effectively limit the amount of violence that the attacking forces may employ against cyber direct participants. On the other hand, individuals who constantly share military intelligence place themselves at an increased risk of being targeted.

In conclusion, given the persistent lack of consensus among States on the matter, the above points raise concerning implications for the ability of IHL in regulating the status and conduct of hacker groups and individuals engaging in cyberspace operations, not only in the context of the Russia-Ukraine armed conflict, but in all future conflicts where civilian participation is enabled by the increased user-friendliness of cyber technologies.

[200] See *supra*, Section 2.6.