ILGSPD Publication Series
No 11/25: Working Paper

The Legal Status of Ukraine's 'IT Army' Volunteers in the Russia-Ukraine Armed Conflict

Tamar Chkhiunidze
November 2025

ERASMUS MUNDUS JOINT MASTER
International Law
of Global Security,
Peace and Development

Erasmus Mundus Joint Master in International Law of Global Security, Peace and Development

International Law of Global Security, Peace and Development (ILGSPD) is a multidisciplinary Master's degree delivered collaboratively by an international consortium composed of six Higher Education institutions: University of Glasgow, Institut Barcelona d'Estudis Internacionals, University of Tartu, Leuphana University of Luneburg, Radboud University, and Université libre de Bruxelles. It is recognised and funded by the European Commission as an Erasmus Mundus Joint Master Degree (EMJMD). The programme provides the next generation of lawyers and policy makers with expert knowledge required to respond to pressing challenges of global security, peace and development and trains tomorrow's leaders to navigate the political context of international law.

ILGSPD Publication Series

ILGSPD Publication Series aims to showcase the work developed by the programme's postgraduate students, in the form of a dissertation, working paper, or policy brief. Publications address themes of global security, peace and development, broadly understood, through the lens of international law, international relations, and/or sustainability.

Coordinating Institution:
University of Glasgow
University Avenue
Glasgow G12 8QQ
Scotland, United Kingdom
E-mail: ilgspd@glasgow.ac.uk
www.globalsecuritylaw-erasmusmundus.eu

The views, information and opinions expressed in this publication are the author's own. The ILGSPD Consortium, or the University of Glasgow, is not responsible for the accuracy of the information.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

Introduction **2**

1. The Legal Status of Ukraine's 'IT Army' Volunteers: Combatants or Civilians? **5**

1.1. 'IT Army' – Regular Armed Force? 5

1.2. 'IT Army' – Irregular Armed Force? 7

1.3. 'IT Army' – *Levée en Masse*? 18

1.4. 'IT Army' – An Organised Armed Group? 22

1.5. 'IT Army' – Civilians Directly Participating in Hostilities? 24

Conclusion **25**

THE LEGAL STATUS OF UKRAINE'S 'IT ARMY' VOLUNTEERS IN THE RUSSIA-UKRAINE ARMED CONFLICT*

*Tamar Chkhitunidze***

Introduction

Over the past two decades, a series of landmark incidents has highlighted the disruptive potential of cyber operations and their growing significance for international security. In 2007, Estonia experienced what was described as 'the first known cyber-attack on an entire country',[1] triggered by the removal of a Soviet-era bronze soldier statue.[2] While focused on legal discussions concerning *jus ad bellum*, this episode underscored a crucial development in cyber operations. In 2008, the Russia-Georgia armed conflict marked 'the first case in history of a coordinated cyberspace domain attack synchronised with major combat actions in the other warfighting domains',[3] raising *jus in bello* issues. Later in 2010, Stuxnet demonstrated the physical destruction potential of cyber operations.[4] In 2015, a British hacker conducting hostile cyber activities for the Islamic State of Iraq and Syria (ISIS) was lethally targeted,[5] marking the first instance where a hacker involved in terrorist cyber operations was considered a legitimate military target.[6]

---

* This paper is the second of a two-part study on civilian participation in cyber warfare during the Russia-Ukraine armed conflict. A companion paper, forming the first part of the study, examines the legal status of Ukraine's mobile app users.

** Tamar Chkhitunidze graduated from the Erasmus Mundus Master's in International Law of Global Security, Peace and Development with a specialisation in International and European Law. Before that, Tamar completed both a Master's degree in International Law and a Bachelor of Laws at Tbilisi State University. Contact email: chkhitunidzetamar@gmail.com.

[1] Damien McGuinness, 'How a Cyber Attack Transformed Estonia' (*BBC*, 27 April 2017) <www.bbc.com/news/39655415> accessed 27 July 2024; See also Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence (CCD COE) 2010) 16 <https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/> accessed 13 June 2024.

[2] Tikk, Kaska and Vihul (n 1) 15–16.

[3] David Hollis, 'Cyberwar Case Study: Georgia 2008' [2011] *Small Wars Journal* 2 <https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf> accessed 25 May 2024; Michael N Schmitt, 'The Law of Cyber Targeting' (2018) 68 Naval War College Review 1.

[4] Stuxnet is a highly complex computer worm. See Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon' (*Wired*, 3 November 2014) <www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 27 July 2024; Sean Watts, 'The Notion of Combatancy in Cyber Warfare' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict. Proceedings 2012* (NATO CCD COE Publications 2012).

[5] Ido Kilovaty, 'ICRC, NATO and the U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law' (2016) 15 Duke Law & Technology Review 1, 2.

[6] ibid.

Against this backdrop, the ongoing armed conflict between Russia and Ukraine stands out as the most digitally integrated conflict to date,[7] marked not only by crowdsourced intelligence through mobile applications[8] but also by the unprecedented creation of the 'IT Army'. More specifically, on February 26, 2022, two days following Russia's full-scale invasion of Ukraine, the Ministry of Digital Transformation of Ukraine announced the formation of Ukraine's 'IT Army',[9] comprising more than 400,000 Ukrainian and international volunteer hackers (hacktivists), engaged in targeting Russian infrastructure and websites.[10] Since its inception, the membership of the 'IT Army's' Telegram channel has gradually decreased. As of November 2025, it has 115,000 subscribers.[11] While not all followers actively contribute to cyber operations (many are there merely to gather information), it is estimated that the 'IT Army' maintains a core of approximately 3,000 to 10,000 active volunteers.[12]

The 'IT Army' of Ukraine identifies itself as a global IT community unified in its resistance against the Russian invasion of Ukraine, with the declared aim of helping Ukraine prevail.[13] The primary method employed by the 'IT Army' is Distributed Denial of Service (DDoS) attacks, which overload websites with traffic to disrupt normal operations. The group has officially claimed responsibility for attacks on various Russian targets.[14]

---

[7] Matthew Ford, 'The Smartphone as Weapon Part 1: The New Ecology of War in Ukraine' (2022) 3 <www.academia.edu/75845985/The_Smartphone_as_Weapon_part_1_the_new_ecology_of_war_in_Ukraine> accessed 30 April 2024; Luke James, 'Military Information Sharing by Ukrainian Citizens in the Digital Environment: DPH? – Blurring of Lines Between Civilian and Military Actors in Ukraine' (*Opinio Juris*, 12 September 2022) <https://opiniojuris.org/2022/09/12/military-information-sharing-by-ukrainian-citizens-in-the-digital-environment-dph-blurring-of-lines-between-civilian-and-military-actors-in-ukraine/> accessed 12 April 2024; Steven Feldstein, 'Disentangling the Digital Battlefield: How the Internet Has Changed War' (*War on the Rocks*, 7 December 2022) <https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/> accessed 12 April 2024.

[8] Examined in detail in the first part of this two-part study. See: Chkhitunidze Tamar, 'The Legal Status of Ukraine's Mobile App Users in the Russia-Ukraine Armed Conflict' (2025).

[9] 'We Are Creating an IT Army - Tweet by Mykhailo Fedorov' (*X (formerly Twitter)*) <https://twitter.com/FedorovMykhailo/status/1497642156076511233> accessed 7 January 2024; 'The Official Website of the IT ARMY of Ukraine' (*IT Army of Ukraine*) <https://itarmy.com.ua/?lang=en> accessed 21 May 2024.

[10] Russell Buchan and Nicholas Tsagourias, 'Ukrainian "IT Army": A Cyber Levée En Masse or Civilians Directly Participating in Hostilities?' (*EJIL: Talk!*, 9 March 2022) <www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/> accessed 6 January 2024; Aiden Render-Katolik, 'The IT Army of Ukraine' <www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine> accessed 7 January 2024; Jennifer Shore, 'Don't Underestimate Ukraine's Volunteer Hackers' (*Foreign Policy*, 12 January 2024) <https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/> accessed 7 January 2024.

[11] 'Official Telegram Chanel of the It Army of Ukraine' (*Telegram*) <https://t.me/s/itarmyofukraine2022> accessed 9 November 2025.

[12] David Kirichenko, 'How Ukraine Built a Volunteer IT Army from Scratch' (*Euromaidan Press*, 15 January 2024) <https://euromaidanpress.com/2024/01/16/how-ukraine-built-a-volunteer-hacker-army-from-scratch/> accessed 30 May 2024.

[13] 'The Official Website of the IT ARMY of Ukraine' (n 9).

[14] IT Army of Ukraine, '"Behold a Masterful Operation Prepared for Nearly a Month" (Telegram Post)' (*Telegram*, 13 March 2024) <https://t.me/itarmyofukraine2022/2041> accessed 29 May 2024 see where the IT Army mentions that 'A multi-faceted attack struck the ticket payment system in Moscow and Kazan by disabling the Troika system, serving 38 regions'; IT Army of Ukraine, '"This Time We Have a Whole Set

Notably, just two days post-formation, the 'IT Army' targeted the Moscow Stock Exchange.[15] Subsequent operations have targeted Russian banks,[16] government websites,[17] food delivery services,[18] and other companies,[19] leading typically to temporary service disruptions.

The shifting landscape of civilian engagement in armed conflicts through digital means raises pivotal questions under International Humanitarian Law (IHL). In International Armed Conflicts (IAC), under IHL, individuals are classified as combatants or civilians.[20] Pursuant to the principle of distinction, civilians are protected from being directly targeted, but this protection can be lost if their actions align with those of combatants, thus making them legitimate targets. Individuals recognised as combatants, members of an organised armed group (OAG), or those directly participating in hostilities (DPH) may become lawful targets.[21]

The present paper intends to address the central question: *In the context of the ongoing Russia-Ukraine armed conflict, what is the legal status of 'IT Army' Volunteers?* The paper adopts a doctrinal legal research methodology. It combines legal analysis of primary sources such as the Third Geneva Convention relative to the Treatment of Prisoners of

---

of Non-Working Internet Providers: Megafon, Chebnet, Wifire, Netbynet" (Telegram Post)' (*Telegram*, 19 March 2024) <https://t.me/itarmyofukraine2022/2067> accessed 29 May 2024 see where the IT Army mentions that 'We hit so beautifully that cable internet fell off across the country, and this is important infrastructure for the economy'; IT Army of Ukraine, '"We Have Never Reached Such Heights Before" (Telegram Post))' (*Telegram*, 25 March 2024) <https://t.me/itarmyofukraine2022/2085> accessed 29 May 2024 see where the IT Army mentions that 'We have never reached such heights before, because "Satellite Communications" and "Gazprom Space Systems" no longer operate after our intervention'; Thomas Brewster, 'Moscow Exchange, Sberbank Websites Knocked Offline - Was Ukraine's Cyber Army Responsible?' (*Forbes*, 28 February 2022) <www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/> accessed 30 May 2024; Daryna Antoniuk, 'Ukrainian Hacktivists Claim to Leak Trove of Documents from Russia's Central Bank' (*The Record from Recorded Future News*, 7 November 2022) <https://therecord.media/ukrainian-hacktivists-claim-to-leak-trove-of-documents-from-russias-central-bank> accessed 30 May 2024.

[15] Brewster (n 14).

[16] IT Army of Ukraine, '"Promsvyazbank, Alfa-Bank, Sberbank, the Electronic Passport System (EPTS), and Rosreestr Were Taken Down by Our Precise Attack" (Telegram Post)' (*Telegram*, 22 May 2024) <https://t.me/itarmyofukraine2022/2191> accessed 2 June 2024; Brewster (n 14); Antoniuk (n 14).

[17] Ministry of Digital Transformation of Ukraine, 'Ministry of Digital Transformation: IT Army Blocks Russian Sites in a Few Minutes - the Main Victories of Ukraine on the Cyber Front' (*Government Portal*, 28 February 2022) <www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti> accessed 16 June 2024.

[18] IT Army of Ukraine, '"Yesterday, for Some Mysterious Reason, Customers of Food Delivery Services Were Unable to Use Them" (Telegram Post)' (*Telegram*, 1 May 2022) <https://t.me/itarmyofukraine2022/320> accessed 6 April 2024; Kyle Fendorf, 'The Dynamics of the Ukrainian IT Army's Campaign in Russia' (*Lawfare*, 15 June 2023) <www.lawfaremedia.org/article/the-dynamics-of-the-ukrainian-it-army-s-campaign-in-russia> accessed 4 June 2024.

[19] IT Army of Ukraine, '"We Have Never Reached Such Heights Before" (Telegram Post))' (n 14).

[20] Nils Melzer explains that these two categories must be 'mutually exclusive, as well as absolutely complementary' to eliminate any ambiguity. See Nils Melzer, 'The Principle of Distinction Between Civilians and Combatants' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (1st edn, Oxford University Press 2014) 297.

[21] For a detailed discussion of the principle of distinction, see the first part of this two-part study.

War (GCIII) and Additional Protocol I to the Geneva Conventions (API) with secondary sources including the International Committee of the Red Cross (ICRC) Interpretive Guidance on the Notion of Direct Participation in Hostilities (ICRC Guidance) and the Tallinn Manual on the International Law Applicable to Cyber Operations (Tallinn Manual).

The paper begins by evaluating whether the 'IT Army' volunteers can be considered part of Ukraine's regular armed forces, reviewing the formal IHL requirements (Section 1.1). It then explores whether the 'IT Army' qualifies as an irregular armed force, examining elements such as belonging to a party to the conflict, command structure, distinctive identification, openly carrying arms, and adherence to IHL (Section 1.2). The paper further explores the potential for recognising 'IT Army' volunteers as participants in *levée en masse*, discussing other relevant conditions such as the temporal and geographical scope, spontaneity of action, and volunteers being inhabitants of unoccupied territory (Section 1.3). Section 1.4 considers whether 'IT Army' could be seen as an organised armed group. The discussion then turns to whether 'IT Army' volunteers can be considered civilians directly participating in hostilities (Section 1.5). Ultimately, the paper concludes that 'IT Army' volunteers do not qualify as combatants, or members of an organised armed group, and their activities generally fall short of constituting DPH. Consequently, they remain civilians and retain their protected status under IHL.

1. The Legal Status of Ukraine's 'IT Army' Volunteers: Combatants or Civilians?

International jurisprudence in cyber warfare is underdeveloped, primarily due to the absence of a specialised legal framework and definitive case law. This challenge extends to the doctrine of combatancy, where legal constructs designed for traditional warfare do not seamlessly apply to cyber warfare. Nevertheless, cyber warfare cannot exist in a legal vacuum. Therefore, until a broader international consensus is achieved, such activities shall be considered within the *lex lata* of IHL.[22]

1.1. 'IT Army' – Regular Armed Force?

IHL recognises as combatants members of regular armed forces, including 'Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces'[23] and 'Members of regular armed forces who

[22] ICRC, 'When Does International Humanitarian Law Apply to the Use of Information and Communications Technologies?' (2023) <www.icrc.org/sites/default/files/wysiwyg/war-and-law/01_when_does_ihl_apply-0.pdf> accessed 18 July 2024; ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2020) 102 International Review of the Red Cross 481; ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper' (ICRC 2019) <www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf> accessed 5 June 2024; David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17 Journal of Conflict and Security Law 279; Nils Melzer, 'Cyberwarfare and International Law' (United Nations Institute for Disarmament Research 2011) <https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 5 June 2024.

[23] Convention (III) Relative to the Treatment of Prisoners of War 1949 art 4(A)(1).

profess allegiance to a government or an authority not recognized by the Detaining Power'.[24] To qualify as a member of the regular armed forces, factors such as the labels applied to units, their organisational structure, the nature of military service (whether compulsory or voluntary), the composition of the military formations, and the status of enlisted individuals (whether they are trained reservists or newly called to active duty) are irrelevant. [25] The key criterion, as Dinstein explains, is whether these units, regardless of designation or structure, form a part of the state's regular armed forces.[26] Thus, the volunteer corps explicitly mentioned in Article 4(A)(1) of the GCIII must be *formally* integrated into the armed forces to fall under the combatant category. Yet, the criteria for inclusion in the armed forces are not delineated by international law and are subject to domestic regulation.[27]

In the cyber domain, operators may be directly incorporated into the armed forces as military cyber units, members of which would qualify as combatants under IHL.[28] An important aspect to note is that the concept of establishing cyber forces had already been mooted in Ukraine in 2021 before the onset of the full-scale invasion.[29] Following the formation of the 'IT Army', Ukraine, in March 2023, accelerated efforts to draft legislation aimed at integrating this volunteer unit into the armed forces.[30] This move was designed to clarify the legal ambiguities surrounding its status.[31] The model Ukraine seeks to emulate is that of Estonia, where volunteer hackers are part of the Cyber Defence Unit within the Estonian Defence League.[32] It is argued that these volunteers would be recognised as combatants in the event of Estonia's involvement in an IAC, as they satisfy the conditions necessary for being considered a part of the armed forces.[33] While Ukraine

[24] ibid 4(A)(3).
[25] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022) 57.
[26] ibid.
[27] *Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War* (1st edn, Cambridge University Press 2021) para 977.
[28] 'International Cyber Law in Practice: Interactive Toolkit' (*Cyber Law Toolkit*, 27 May 2024) <https://cyberlaw.ccdcoe.org/wiki/Main_Page> accessed 28 May 2024.
[29] National Security and Defense Council of Ukraine, 'О. Данілов провів нараду з питань створення кібервійськ [O. Danilov Held a Meeting on the Creation of Cyber Forces]' (*Рада національної безпеки і оборони України*, 13 September 2021) <www.rnbo.gov.ua/ua/Diialnist/4995.html> accessed 29 May 2024.
[30] Shaun Waterman, 'Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army' (*Newsweek*, 14 March 2023) <www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814> accessed 15 May 2024.
[31] ibid.
[32] ibid; Sofia Yelagina, 'Законопроєкт Про Кіберсили ЗСУ Вже Обговорюють у МО Та Силах Оборони. Ми Дізнались Більше Про Майбутній Рід Військ [The Draft Law on the Cyber Forces of the Armed Forces of Ukraine Is Already Being Discussed in the Ministry of Defense and the Defense Forces. We Learned More About the Future Branch of the Military]' (*AIN.Capital*, 8 May 2024) <https://ain.ua/2024/05/08/cyberforce/> accessed 29 May 2024.
[33] Kadri Kaska, Anna-Maria Osula and Jan Stinissen, 'The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis' 35 <https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/> accessed 29 May 2024.

has enacted additional legislation to enhance its cyber defences,[34] as of November 2025, the legislative process for the Cyber Forces of the Armed Forces of Ukraine is still ongoing.[35]

Several key points emerge from this discussion. Firstly, the law required to formally incorporate the 'IT Army' into the Ukrainian armed forces has not yet been adopted. Consequently, as it stands, the 'IT Army' volunteers do not fulfil the requirements for combatant status as defined by Article 4(A)(1) of the GCIII. Moreover, even after the law's potential enactment, the incorporation of volunteer corps into the armed forces, while governed by domestic law, shall not be applied retroactively.[36] Therefore, actions undertaken by the 'IT Army' volunteers before their formal incorporation into the Ukrainian armed forces must not be regarded as those of combatants.

Another aspect to consider is that the Head of the Information Security and Cybersecurity Service of the National Security and Defence Council of Ukraine has discussed the establishment of a cyber reserve and the engagement of cyber volunteers.[37] The determination of whether reservists constitute members of the armed forces of a party to the conflict is also contingent upon domestic law.[38] However, even if Ukraine establishes such a reserve under domestic legislation, only reservists who are called to active duty will be considered members of the armed forces under the provisions of Article 4(A)(1).[39]

This analysis indicates that, at the present moment, under IHL, the 'IT Army' volunteers do not qualify for combatant status under Article 4(A)(1) of the GCIII as members of regular armed forces. Should Ukraine adopt the relevant legislation and incorporate the voluntary unit into its armed forces, its members could be considered combatants, similar to the Estonian volunteer hackers. However, only actions undertaken by the 'IT Army' volunteers after their formal incorporation into the Ukrainian armed forces must be regarded as those of combatants. With this in mind, we can now move to discuss whether, as of now, 'IT Army' volunteers can be considered members of irregular armed forces.

1.2. 'IT Army' – Irregular Armed Force?

As previously mentioned, combatant status extends beyond regular armed forces. IHL also recognises as combatants members of irregular armed forces, including 'Members of other militias and members of other volunteer corps, including those of organized

---

[34] Militarnyi, 'Президент підписав закон про електронний кабінет військовозобов'язаного [President Signed the Law on the Electronic Cabinet of Persons Liable for Military Service]' (*Мілітарний*, 2 April 2024) <https://mil.in.ua/uk/news/prezydent-pidpysav-zakon-pro-elektronnyj-kabinet-vijskovozobov-yazanogo/> accessed 29 May 2024.
[35] 'Проект Закону Про Кіберсили Збройних Сил України [Draft Law on Cyber Forces of the Armed Forces of Ukraine]' (*Verkhnova Rada of Ukraine*) <https://itd.rada.gov.ua/billInfo/Bills/Card/45453> accessed 9 November 2025.
[36] *Commentary on the Third Geneva Convention* (n 27) para 977.
[37] Yelagina (n 32).
[38] *Commentary on the Third Geneva Convention* (n 27) para 977.
[39] ibid.

resistance movements, *belonging* to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied'.[40] These groups must meet the following cumulative requirements for their members to qualify for combatant and POW status:[41]

a. Belonging to Ukraine;
b. Commanded by a person responsible for their subordinates;
c. Wearing a fixed distinctive sign recognisable at a distance;
d. Carrying arms openly; and
e. Conducting operations in accordance with the laws and customs of war.

Therefore, even with a less formal association with a party to the conflict, volunteers of the 'IT Army' could still qualify as combatants if they satisfy the aforementioned criteria and belong to Ukraine as understood under Article 4(A)(2) of the GCIII.

1.2.1. Belonging to Ukraine

First and foremost, the 'IT Army' must be affiliated with the party to the conflict – Ukraine. The term 'belonging to' in Article 4(A)(2) of the GCIII outlines the relationship that irregular armed forces and a party to a conflict must maintain for the group's members to gain combatant status.[42] The criteria for a group to belong to the state involve establishing a *de facto* relationship.[43] This requires that 1) the group actively engages in combat on behalf of that party, and 2) the party must formally recognise the group's combat role and affirm that the combat activities are conducted in its interests.[44]

On its official website, the 'IT Army' of Ukraine describes itself as 'a worldwide IT community united to resist the Russian invasion of Ukraine' and states its goal 'to help Ukraine win'.[45] The group has also officially claimed responsibility for attacks on various Russian targets,[46] which aligns with the criterion of fighting on behalf of Ukraine, thus meeting this requirement should not pose a problem. However, it might be more

[40] Convention (III) Relative to the Treatment of Prisoners of War (n 23) art 4(A)(2) (emphasis added).
[41] ibid.
[42] *Commentary on the Third Geneva Convention* (n 27) para 1004.
[43] ibid.
[44] ibid 1005.
[45] 'The Official Website of the IT ARMY of Ukraine' (n 9).
[46] IT Army of Ukraine, '"Behold a Masterful Operation Prepared for Nearly a Month" (Telegram Post)' (n 14) see where the IT Army mentions that 'A multi-faceted attack struck the ticket payment system in Moscow and Kazan by disabling the Troika system, serving 38 regions'; IT Army of Ukraine, '"This Time We Have a Whole Set of Non-Working Internet Providers: Megafon, Chebnet, Wifire, Netbynet" (Telegram Post)' (n 14) see where the IT Army mentions that 'We hit so beautifully that cable internet fell off across the country, and this is important infrastructure for the economy'; IT Army of Ukraine, '"We Have Never Reached Such Heights Before" (Telegram Post))' (n 14) see where the IT Army mentions that 'We have never reached such heights before, because "Satellite Communications" and "Gazprom Space Systems" no longer operate after our intervention'; Brewster (n 14); Antoniuk (n 14).

challenging to determine whether a state officially recognises the group's combat role and accepts that the actions are conducted on its behalf.

According to the commentary for Article 4(A)(2) of the GCIII, such acceptance can manifest in various forms[47] – it may be explicit, such as through formal acknowledgement, or implicit, indicated by the state's actions that it recognises the group is fighting on its behalf.[48] In this specific instance, Ukraine not only publicly announced the formation of the 'IT Army' but also has not denied that the 'IT Army' operates on its behalf. On the contrary, reports suggest that although the 'IT Army' functions independently from the government, the government has reached out to it for assistance when necessary.[49] Furthermore, Ukraine has recognised and even awarded hackers from a team that was established with the assistance of the 'IT Army',[50] further supporting its endorsement of the group's activities. This suggests a level of acceptance and acknowledgement of the 'IT Army's' role and actions as being on behalf of Ukraine.

Following on from this, the Tallinn Manual provides a relevant example where a state might engage a group of private individuals for cyber operations during an armed conflict due to their unique capabilities or knowledge that state organs lack.[51] Under these conditions, and as long as the group aligns with the state's objectives and meets other established criteria of combatancy, its members would be entitled to combatant status.[52] Given this context, where the 'IT Army' is recognised by Ukraine, it is essential to further examine the additional requirements for combatant status to definitively establish their standing under IHL.

For the 'IT Army' volunteers to be regarded as combatants, the group, besides belonging to a party to the conflict, must also satisfy four cumulative criteria. These are: being commanded by a person responsible for their subordinates, wearing a fixed distinctive sign recognisable at a distance, carrying arms openly, and conducting operations under the laws and customs of war.[53] The extent to which the 'IT Army' meets each of these criteria is analysed below.

---

[47] *Commentary on the Third Geneva Convention* (n 27) para 1006.
[48] ibid 1006–1007.
[49] Kirichenko (n 12).
[50] Joe Tidy, 'Ukraine Gives Award to Foreign Vigilantes for Hacks on Russia' (*BBC*, 3 April 2024) <www.bbc.com/news/technology-68722542> accessed 30 May 2024; 'The Official Website of Team Onefist' (*Team Onefist*) <www.onefist.org> accessed 30 May 2024; IT Army of Ukraine, '"A Big Thank You to the Ministry of Digital Transformation @FedorovMykhailo for Recognizing Our Relentless Efforts and Recent Successes."' (*X (formerly Twitter)*, 11 October 2023) <https://x.com/ITArmyUKR/status/1712107660454105172?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1712107660454105172%7Ctwgr%5Eee68da5a84a5ff9accf1b3c1a26fe67c77ab40f7%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Ftherecord.media%2Fukraine-volunteer-it-army-machine-low-level-attacks> accessed 2 June 2024.
[51] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) r 87 para 8.
[52] ibid.
[53] Convention (III) Relative to the Treatment of Prisoners of War (n 23) art 4(A)(2).

1.2.2. Command Structure

The requirement for a group to be commanded by an individual responsible for their subordinates fundamentally relates to the organisational structure of the group.[54] This stipulation is crucial as a well-defined hierarchy facilitates the enforcement of internal discipline and ensures that operations are executed in a manner that aligns with IHL.[55] Indications of responsible command within a group might include regular involvement in the planning and execution of military operations, overseeing training activities, and enforcing discipline among subordinates.[56] While the command framework does not need to be 'sophisticated or rigid',[57] the absence of a structured command could significantly undermine a group's claim to combatant status.[58]

The Tallinn Manual specifically notes that organisation primarily through virtual means is likely insufficient for a group to be recognised as a volunteer corps eligible for combatant status, underscoring the challenges a purely online entity faces in meeting this criterion.[59] This is corroborated by the 'IT Army's' situation. The available information remains sparse, yet some 'IT Army' volunteers have mentioned a certain level of coordination and the existence of multiple units within the organisation.[60] However, there is no identification of a single leader for the group.[61] The absence of a distinct leader indicates that the group lacks the necessary level of organisation and, consequently, does not satisfy the criterion of having a responsible command.

1.2.3. Distinctive Identification

Regarding the criterion of wearing a fixed distinctive sign recognisable at a distance, the commentary on the GCIII states that such a sign should not be easily removed or hidden 'at the first sign of danger'.[62] It must enable the identification of the person as a member of the volunteer corps, ensuring they are not mistaken for civilians or members of the enemy forces.[63] Nonetheless, there is a degree of flexibility inherent in the interpretation of this provision, assessing whether a combatant is 'wearing a fixed distinctive emblem' is necessarily context-specific.[64]

---

[54] *Commentary on the Third Geneva Convention* (n 27) para 1013; *Tallinn Manual* (n 51) r 87 para 10.
[55] *Commentary on the Third Geneva Convention* (n 27) para 1013.
[56] ibid 1014.
[57] ibid.
[58] *Tallinn Manual* (n 51) r 87 para 10.
[59] ibid.
[60] Kirichenko (n 12); Daryna Antoniuk, 'How Ukraine's Volunteer Hackers Have Created a "Coordinated Machine" Around Low-Level Attacks' (*The Record from Recorded Future News*, 4 April 2024) <https://therecord.media/ukraine-volunteer-it-army-machine-low-level-attacks> accessed 28 May 2024.
[61] Antoniuk (n 60).
[62] *Commentary on the Third Geneva Convention* (n 27) para 1016.
[63] ibid 1017–1018.
[64] ibid 1018; Dinstein (n 25) 61.

In the cyber domain, it is argued that the relevance of this requirement is considerably reduced.[65] While the Tallinn Manual maintains that those engaged in cyber operations must not deviate from wearing a distinctive emblem, regardless of their physical distance from the battlefield or separation from civilian areas,[66] this perspective is contentious. Others argue that when there is no risk of deception or confusion with civilians, the necessity for a combatant to wear a distinguishing emblem becomes redundant.[67] These experts argue for an exception to the requirement of wearing a distinctive sign, citing customary international law.[68] They provide an example where a Special Forces team must identify and attack a military cyber control facility among similar civilian facilities.[69] These experts contend that, in such cases, the absence of uniforms among military personnel may increase the risk of mistakenly targeting civilian sites.[70] However, this rationale does not hold where the absence of a distinctive sign does not impact the Special Forces' ability to carry out their task.[71] With no definitive position on this issue, both perspectives hold equal weight. Therefore, while the latter approach appears more feasible, a stringent standard should be applied to assess the 'IT Army' volunteers' adherence to this criterion. According to the stringent standards of the Tallinn Manual, the 'IT Army' does not satisfy this criterion, as there is no documented evidence that the 'IT Army' volunteers distinguish themselves with a 'fixed distinctive sign recognisable at a distance'.

1.2.4. Carrying Arms Openly

In traditional kinetic warfare, carrying arms openly implies the visible bearing of weapons without any concealment.[72] In determining whether computers or other cyber means can be considered weapons, it is useful to reflect on the broader definitions provided by international legal precedents. The International Court of Justice (ICJ), in its *Advisory Opinion on Nuclear Weapons*, asserted that any instrument causing harmful effects could be categorised as a weapon.[73] Extending this principle to cyber operations, the Tallinn Manual offers a detailed definition, characterising cyber weapons as those means of cyber warfare specifically used, designed, or intended to inflict injury or death on persons, or to cause damage or destruction to objects.[74] Such definitions imply that the designation of cyber means as weapons hinges on their intended use in conducting

[65] Giacomo Biggio, 'The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict' [2024] Journal of International Humanitarian Legal Studies 1, 160–164.
[66] *Tallinn Manual* (n 51) r 87 para 11.
[67] ibid paras 12–13; Heather Harrison Dinniss, *Cyberwarfare and the Laws of War* (1st edn, Cambridge University Press 2012) 148 as cited in; Biggio (n 65) 161; Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50 Virginia Journal of International Law 391, 440.
[68] *Tallinn Manual* (n 51) r 87 para 12.
[69] ibid.
[70] ibid.
[71] ibid.
[72] *Commentary on the Third Geneva Convention* (n 27) para 1021.
[73] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* [1996] ICJ Reports (International Court of Justice) [39].
[74] *Tallinn Manual* (n 51) r 103 para 2.

cyber-attacks, encompassing a wide array of devices, materials, instruments, mechanisms, equipment, or software if employed for these purposes.[75]

In the realm of cyber warfare, the criterion of carrying arms openly encounters critiques similar to those regarding the wearing of a distinctive sign. Scholars and the Tallinn Manual largely concur on this point, indicating that the literal interpretation of 'carrying arms openly' may lead to impractical outcomes in a cyber context.[76] The Tallinn Manual further elaborates that this requirement holds minimal relevance in cyber operations, where the visibility of weaponry is not applicable in the same way as in conventional conflicts.[77] Although at times a computer may be classified as a 'weapon', the mere possession of such a device cannot automatically imply engagement in combatant activities.[78] It has been suggested that an effective method for satisfying the requirement to carry arms openly in cyber warfare involves ensuring that operatives do not falsely represent themselves as protected, non-combatant entities.[79] This means, for example, avoiding the use of computers or networks of hospitals or schools for initiating cyber-attacks, thereby steering clear of acts of perfidy.[80] Although no such incident has been documented, the debate persists, and it remains a contentious point to assert that 'IT Army' volunteers carry arms openly. The present paper supports the view that this criterion should not be interpreted literally. However, as with the criterion for wearing a distinctive sign, considering the stringent standard, 'IT Army' volunteers do not meet the criterion of carrying arms openly.

1.2.5. Adherence to IHL

Regarding the requirement for adherence to IHL, although there is some disagreement among scholars,[81] the prevailing view is that collective actions, rather than individual behaviours, are decisive in determining eligibility for combatant status.[82] Systematic or large-scale breaches of IHL by the group as a whole could lead to disqualification, but isolated instances of non-compliance by individual members typically do not impact the status of the entire group.[83]

While the total number of operations by the 'IT Army' remains uncertain, it is believed that around 2,240 targets (impacting over 15,000 online resources) had been attacked by

[75] ibid.
[76] Watts (n 67) 440; Biggio (n 65) 160–164; Harrison Dinniss (n 67) 145, 148; *Tallinn Manual* (n 51) r 87 para 14.
[77] *Tallinn Manual* (n 51) r 87 para 14.
[78] David Wallace and Shane Reeves, 'The Law of Armed Conflict's "Wicked" Problem: Levee En Masse in Cyber Warfare' (2013) 89 International Law Studies 646, 659.
[79] Melzer, 'Cyberwarfare and International Law' (n 22) 34; Christopher Waters, 'New Hacktivists and the Old Concept of Levée En Masse' (2014) 37 The Dalhousie Law Journal 771, 783–784.
[80] Waters (n 79) 784.
[81] Dinstein (n 25) 68.
[82] *Commentary on the Third Geneva Convention* (n 27) para 1026; *Tallinn Manual* (n 51) r 87 para 15.
[83] *Commentary on the Third Geneva Convention* (n 27) para 1026; *Tallinn Manual* (n 51) r 87 para 15.

February 2023.[84] Although tracking each operation does not seem feasible, an overarching understanding can be pieced together from the publicly available information on some of their most significant targets.

Just two days post-formation, the 'IT Army' targeted the Moscow Stock Exchange, marking its first strike against civilian infrastructure.[85] Contrary to initial assertions that only military targets would be engaged,[86] the 'IT Army' broadened its focus to include dual-use infrastructure such as Russia's homegrown satellite-based navigation system, GLONASS,[87] and civilian targets, including banking[88] and food delivery sectors.[89] These actions have sparked scholarly debate and accusations of the 'IT Army' engaging in indiscriminate and deliberate targeting of civilian infrastructures.[90] This pattern of cyber warfare, observed on both sides of the conflict, prompted the ICRC to issue the first-ever set of rules for civilian hackers.[91] Following this, the 'IT Army' has committed to moderating its cyber operations and adhering to these rules of engagement.[92] However, instances involving the targeting of civilian infrastructure have persisted.[93]

While Article 4(A)(2) of GCIII mandates that 'operations' must comply with the laws and customs of war, in practice, the stringent legal restraints of IHL – specifically the principles of distinction, proportionality, and precautions – only apply to those operations that are deemed 'attacks' according to IHL definitions.[94] However, it is important to note that not

---

[84] Ministry of Digital Transformation, 'Підсумки Роботи ІТ-Армії. Як Українські ІТ-Волонтери Забезпечували Кіберфронт [Results of the Work of the IT Army. How Ukrainian IT Volunteers Provided the Cyber Front] (Telegram Post)' (*Telegram*, 20 February 2023) <https://t.me/mintsyfra/3834> accessed 2 June 2024.
[85] Brewster (n 14).
[86] The Associated Press, 'Ukraine Cyber Official: We Only Attack Military Targets' (*The Independent*, 4 March 2022) <www.independent.co.uk/news/ukraine-russia-kremlin-boston-hackers-b2028853.html> accessed 4 June 2024.
[87] James Pearson, 'Ukraine's "IT Army" Targets Belarus Railway Network, Russian GPS' (*Reuters*, 3 March 2022) <www.reuters.com/world/europe/ukraines-it-army-targets-belarus-railway-network-russian-gps-2022-03-03/> accessed 4 June 2024.
[88] IT Army of Ukraine, '"Promsvyazbank, Alfa-Bank, Sberbank, the Electronic Passport System (EPTS), and Rosreestr Were Taken Down by Our Precise Attack" (Telegram Post)' (n 16).
[89] IT Army of Ukraine, '"Yesterday, for Some Mysterious Reason, Customers of Food Delivery Services Were Unable to Use Them" (Telegram Post)' (n 18); Fendorf (n 18).
[90] Stefan Soesanto, 'The IT Army of Ukraine: Structure, Tasking, and Ecosystem' (Center for Security Studies (CSS), ETH Zürich 2022) 4; Stefan Soesanto, 'Ukraine's Counter-Hybrid Campaigns in Cyberspace' (The Hague Centre for Strategic Studies 2023) 10; Stefan Soesanto, 'Ukraine's IT Army' (2023) 65 Survival 93, 97; Fendorf (n 18); Jason Healey and Olivia Grinberg, '"Patriotic Hacking" Is No Exception' (*Lawfare*, 27 September 2022) <www.lawfaremedia.org/article/patriotic-hacking-no-exception> accessed 5 June 2024.
[91] Tilman Rodenhäuser and Mauro Vignati, '8 Rules for "Civilian Hackers" During War, and 4 Obligations for States to Restrain Them' (*Humanitarian Law & Policy*, 4 October 2023) <https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/> accessed 4 June 2024.
[92] Joe Tidy, 'Ukraine Cyber-Conflict: Hacking Gangs Vow to De-Escalate' (*BBC*, 6 October 2023) <www.bbc.com/news/technology-67029296> accessed 4 June 2024.
[93] IT Army of Ukraine, '"Promsvyazbank, Alfa-Bank, Sberbank, the Electronic Passport System (EPTS), and Rosreestr Were Taken Down by Our Precise Attack" (Telegram Post)' (n 16).
[94] ICRC, 'ICRC Position Paper' (n 22) 7; *Tallinn Manual* (n 51) r 94 para 3, r 99 para 3.

every cyber operation reaches the threshold necessary to be deemed an attack.[95] Currently, there is an ongoing debate about whether only cyber operations that meet the definition of an 'attack' should trigger the applicability of IHL rules, or if operations that do not reach this attack threshold should also be considered. To accurately classify the operations of the 'IT Army' and assess their compliance with IHL, it is crucial to first determine the criteria under which cyber operations are categorised as attacks. Understanding this threshold will clarify where the activities of the 'IT Army' fall within these definitions.

1.2.5.1. Do 'IT Army's' Cyber Operations Constitute 'Attacks' under IHL?

While the principle of distinction typically refers to 'military operations',[96] it is primarily meant to address 'attacks' as defined under IHL.[97] Article 49(1) of the API defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. This clarifies that the element of violence is what distinguishes attacks from other military operations, emphasising that the essence of an attack is determined by the effects it causes.[98] The term 'acts of violence' is now widely accepted to include not only physical force but also cyber operations (although not all of them) that can rise to this level.[99] The challenge in defining the application of cyber operations is compounded not only by the lack of clear guidance within existing laws but also by the absence of a consensus among states on this matter.[100]

A fundamental consensus among virtually all stakeholders is that any cyber operation leading foreseeably to physical damage or destruction, or to injury or death, clearly constitutes an 'attack' under the definition provided in Article 49(1) of the API.[101] Yet, this

---

[95] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (2015) 32IC/15/11 41–42 <www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf> accessed 7 June 2024; *Tallinn Manual* (n 51) r 92 para 14.
[96] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict 1977 art 48.
[97] Michael N Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict. Proceedings 2012* (NATO CCD COE Publications, 2012 2012) 289; Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 Naval War College International Law Studies 89, 91–92; Some argue that even non-violent operations, which do not amount to attacks, should still be limited to military objectives. See Harrison Dinniss (n 67) 200.
[98] *Tallinn Manual* (n 51) r 92 paras 2–3.
[99] ibid para 3; Schmitt, 'Cyber Operations and the Jus in Bello' (n 97) 93–94; Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533, 557; Laurent Gisel and Lukasz Olejnik, 'The Potential Human Cost of Cyber Operations' (2019) ICRC Expert Meeting.
[100] Robin Geiss and Henning Lahmann, 'Protecting Societies: Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (The Geneva Academy of International Humanitarian Law and Human Rights 2021) 9–10 <www.adh-geneve.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf> accessed 5 June 2024.
[101] Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102 International Review of the Red Cross 287, 312–313; *Tallinn Manual* (n 51) r 92.

offers little insight into our case since no reports suggest that operations conducted by the 'IT Army' have led to such direct physical consequences.

Beyond this widely accepted view of the 'kinetic-equivalence effects test',[102] opinions diverge on whether a cyber operation that incapacitates an object without causing physical damage constitutes an attack under IHL.[103] This topic sparked considerable debate during the drafting of the Tallinn Manual. A majority of the experts concluded that a cyber operation should be considered an attack if it disrupts functionality to the extent that physical components must be replaced to restore it.[104] Additionally, some experts argue that an operation should also qualify as an attack if restoring functionality requires reinstalling the operating system or specific data.[105]

The ICRC adopts a broader interpretation, advocating that any operation aimed at disabling a computer or computer network during armed conflict should be considered an attack under IHL, irrespective of whether the disablement involves physical destruction or occurs through other means.[106] According to the ICRC, this interpretation aligns with the definition of military objectives in Article 52(2) of the API, which includes 'neutralization' – impairing functionality – alongside physical damage or destruction as outcomes of an attack.[107] The ICRC holds that a narrow definition of 'attack' would conflict with the intent and purpose of the rules of hostilities, which aim to protect civilian populations and objects from the effects of hostilities.[108] The ICRC further highlights that a narrow interpretation of cyber operations could leave civilian infrastructures such as electricity, banking, and communications without adequate legal protection under IHL, exposing civilians and their essential services to cyber-attacks without sufficient legal safeguards.[109] This broader interpretation is shared by some scholars who also contend that an inclusive definition of 'attack' is necessary to ensure comprehensive protection for civilians and civilian objects in the context of modern warfare, particularly in cyber operations.[110] However, there are opposing views arguing that this broad interpretation risks 'overinclusivity', potentially classifying a wide range of cyber operations as attacks.[111]

---

[102] Karine Bannelier, 'Is the Principle of Distinction Still Relevent in Cyberwarfare?' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 348 as cited in; Biggio (n 65) 154.
[103] *Tallinn Manual* (n 51) r 92 paras 10–12.
[104] ibid para 10.
[105] ibid para 11.
[106] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95) 41; ICRC, 'ICRC Position Paper' (n 22) 7–8.
[107] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95) 41.
[108] ibid.
[109] ibid; ICRC, 'ICRC Position Paper' (n 22) 8.
[110] Geiss and Lahmann (n 100); Ido Kilovaty, 'Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law' (2016) 23 Michigan Telecommunications & Technology Law Review 113; Droege (n 99) 559 See also.
[111] Schmitt, 'Cyber Operations and the Jus in Bello' (n 97) 95; Droege (n 99) 559–560; Melzer, 'Cyberwarfare and International Law' (n 22) 26.

It is apparent that despite the instrumentality-based definition of 'attack' – which focuses on the means and methods used to carry out the attack rather than the direct violent impact itself – IHL employs a consequence-based approach in its practical application, ensuring that the focus remains on the harmful effects caused by the attack.[112] To further distinguish operations that qualify as attacks from those that do not, the concept of 'inconvenience' has been suggested as a criterion based on the effects of an operation.[113] However, the term 'inconvenience' lacks a specific definition within IHL, which introduces ambiguity in interpreting and applying IHL to various cyber operations, highlighting a gap in the framework that might necessitate further clarification to ensure consistent application. As Droege points out, while there may be general agreement that the disruption of an online booking system constitutes merely an inconvenience, achieving consensus on issues such as interference with banking services proves more challenging.[114]

The Ukrainian DDoS attacks have generally led to temporary disruptions. Over time, affected servers are restored, defences are improved, and the impact of subsequent attacks diminishes.[115] Whether these DDoS attacks meet the threshold of an 'attack' under IHL remains debatable.

If we adopt the broader interpretation suggested by the ICRC, even cyber operations that qualify as 'military operations' without necessarily constituting 'attacks' *per se* would still be governed by the principle of distinction.[116] This broader definition would encompass all forms of DDoS attacks, including those that cause mere inconvenience, such as blocking a television broadcast,[117] and thus would include the 'IT Army's' cyber operations. However, it is argued that extending the notion of 'attack' to cover any DDoS attack, such as those targeting food delivery services, may be excessive.[118] State practice does not support the idea that causing mere inconvenience is intended to be prohibited under IHL.[119] As suggested, if the disruption caused by a cyber operation is only temporary and requires no repair, it would not meet the definition of an 'attack' as understood in IHL.[120] Therefore, such operations would not be subject to the applicable

[112] Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' (n 97) 291.
[113] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95) 42; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 181.
[114] Droege (n 99) 560.
[115] As reported the longest DDoS attack lasted for over a week. See Matt Burgess, 'Russia Is Being Hacked at an Unprecedented Scale' (*Wired*, 27 April 2022) <www.wired.com/story/russia-hacked-attacks/> accessed 12 June 2024.
[116] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95) 42.
[117] IT Army of Ukraine, 'We Launched a DDoS Attack on Channels Showing Putin's Address to the Federal Assembly: 1TV, VGTRK and SMOTRIM (Telegram Post)' (*Telegram*, 21 February 2023) <https://t.me/itarmyofukraine2022/1054> accessed 7 June 2024.
[118] Melzer, 'Cyberwarfare and International Law' (n 22) 26; Droege (n 99) 559–560.
[119] Schmitt, 'Cyber Operations and the Jus in Bello' (n 97) 95.
[120] Michael N Schmitt, 'France Speaks Out on IHL and Cyber Operations: Part II' (*EJIL: Talk!*, 1 October 2019) <www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/> accessed 7 June 2024.

IHL rules, regardless of whether the target is classified as a military objective. Thus, under this narrow definition, the 'IT Army's' cyber operations would comply with IHL.

As with the criteria for wearing a distinctive sign and carrying arms openly, there is no universally agreed-upon approach to this issue. The present paper shares the latter opinion that the definition should be applied strictly. While the ICRC's definition is deemed ideal, it is less applicable in practice as it is not supported by state practice. Even if it were assumed that the 'IT Army' meets all the contentious requirements for combatant status (wearing distinctive insignia, carrying arms openly and complying with IHL rules), they still lack at least one crucial element: being under responsible command. This requirement is fundamental for classifying members of a group as combatants, and without it, the 'IT Army' volunteers cannot currently be considered as such. This analysis indicates that, under IHL, the 'IT Army' volunteers do not qualify for combatant status under Article 4(A)(2) of the GCIII as members of irregular armed forces.

1.2.6. Interpretations of the Additional Protocol I

Building on the conclusion that the 'IT Army' does not meet the combatant criteria under Article 4(A)(1) and (2) of the GCIII, it is important to consider their status within the broader provisions of the API, to which both Ukraine and Russia are parties. The API revises the traditional classifications of combatants by removing the distinction between regular and irregular forces.[121] According to Article 43 of the API, combatants are defined as members of the 'armed forces of a Party to a conflict', which includes all organised armed forces, groups, and units that are under a command responsible to that party for the conduct of its subordinates.[122] Additionally, the API mandates that these forces 'shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict'.[123]

Furthermore, Article 44(3) of the API modifies the conditions for combatancy in specific circumstances, typically seen in wars of national liberation or occupied territories. It relaxes traditional requirements such as the need for a distinctive emblem or the open carrying of arms.[124] Despite these relaxations, the fundamental requirements for combatancy – such as being under a responsible command – still apply. The 'IT Army's' failure to meet this essential command structure requirement excludes them from combatant status under the API, just as it does under GCIII. Moreover, Article 44(6) of the API offers a safeguard, stating that non-fulfilment of the API's conditions does not compromise the combatant status that may have been attained under Article 4 of GCIII.[125]

---

[121] *Commentary on the Third Geneva Convention* (n 27) para 1009; Knut Ipsen, 'Combatants and Non-Combatants' in Dieter Fleck and Michael Bothe (eds), *The handbook of international humanitarian law* (Fourth edition, Oxford University Press 2021) 100.
[122] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 96) art 43(1), 43(2).
[123] ibid 43(1).
[124] ibid 44(3).
[125] *Commentary on the Third Geneva Convention* (n 27) para 1009.

This provision ensures that while the API offers a more lenient approach in certain areas, the core criteria for combatancy and the protections afforded by GCIII are not diluted. Thus, even though in general the API appears more accommodating than GCIII, it ultimately upholds similar stringent standards for determining combatant status. The analysis concludes that while 'IT Army' volunteers do not qualify for combatant status as members of irregular armed forces, they may still be recognised as combatants if considered participants in a *levée en masse*. The next section explores this possibility in detail.

1.3. 'IT Army' – *Levée en Masse*?

Should 'IT Army' volunteers not satisfy the criteria for classification as combatants under the frameworks of regular or irregular armed forces as delineated in Article 4(A)(1) and 4(A)(2) of the GCIII, there remains the possibility for them to be recognised as combatants under the concept of *levée en masse*.

Article 4(A)(6) of the GCIII delineates specific conditions under which participants in a *levée en masse* are recognised. These participants are defined as:

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

Thus, to qualify as *levée en masse* these individuals shall:

a. Act during the invasion phase of the conflict;
b. Form spontaneously and operate in an unorganised manner under emergency conditions;
c. Be residents of the invaded territory;
d. Remain within the geographic confines of unoccupied territory;
e. Carry weapons openly; and
f. Adhere to the laws and customs of war.

This classification does not necessitate formal organisation or an established link – either *de jure* or *de facto* – with a belligerent party. Moreover, participants in such a scenario are not obliged to be under the command of a responsible officer, nor are they required to wear a distinctive sign that is recognisable from a distance.[126]

However, to be classified as a cyber *levée en masse*, certain specific conditions set out in Article 4(A)(6) of GCIII must be met. Given the rarity of conflicts that could justify a cyber *levée en masse* and the narrow circumstances under which civilians might be deemed

[126] Convention (III) Relative to the Treatment of Prisoners of War (n 23) art 4(A)(6); *Tallinn Manual* (n 51) r 88 para 2; Dinstein (n 25) 68; Wallace and Reeves (n 78) 656–657.

participants at such a scale, it is crucial to explore to what extent the 'IT Army' aligns with these stipulated conditions. This discussion is essential in understanding the applicability of traditional combatant definitions to contemporary forms of cyber warfare, where conventional criteria may not seamlessly apply. To explore these conditions in the context of cyber warfare and assess their applicability to the 'IT Army' volunteers, this section considers several key aspects.

1.3.1. Temporal Scope

Article 4(A)(6) of GCIII restricts the recognition of combatant status to the precise time frame of the actual invasion period. According to the commentary of the GCIII, if the resistance extends beyond this initial period, allowing time for the inhabitants to organise into more structured, regular armed units, then the relevance of Article 4(A)(6) diminishes and no longer applies to these more organised fighters.[127] However, IHL does not stipulate a definitive period within which the inhabitants of a non-occupied territory are required to organise into regular armed units.[128] This ambiguity raises questions about whether groups, such as the 'IT Army', have had adequate time to align themselves with the stipulations of Article 4(A)(2) of the GCIII.

Reports indicate that the 'IT Army' remains unstructured. However, this likely reflects a deliberate choice rather than an absence of opportunity. Three years post-establishment, it is reasonable to conclude that there has been ample time for the 'IT Army' to evolve into a more organised entity if that had been the intention. Moreover, the Ukrainian government had initiated legislation aimed at formally incorporating this volunteer group into its armed forces well before this period,[129] suggesting recognition and a pathway for such formalisation.

1.3.2. Spontaneity

Spontaneity under Article 4(A)(6) dictates that only individuals who react instantaneously to the immediate threat of an invading force – without prior organisation by state mechanisms – are eligible for consideration under certain legal protections.[130] This spontaneity criterion is not predicated on the element of surprise, it remains applicable even to those forewarned of an approaching enemy.[131] The essential issue then becomes whether the group has been formally organised by the government of the invaded country.[132] There is no evidence suggesting that the government itself organised the 'IT Army'. Although the Ukrainian government announced the creation of the 'IT Army'

[127] *Commentary on the Third Geneva Convention* (n 27) para 1064.
[128] David Wallace and Shane Reeves, 'Levée En Masse in Ukraine: Applications, Implications, and Open Questions' (*Lieber Institute*, 11 March 2022) <https://lieber.westpoint.edu/levee-en-masse-ukraine-applications-implications-open-questions/> accessed 9 June 2024.
[129] Waterman (n 30); Yelagina (n 32).
[130] *Commentary on the Third Geneva Convention* (n 27) para 1066.
[131] ibid.
[132] Buchan and Tsagourias (n 10).

and acknowledges its actions as being on behalf of Ukraine, as discussed in subsection 1.3.1, this does not amount to a formal organisation. While this may be viewed as an invitation or encouragement, it is argued that mere encouragement or directives from a state, even if they include specific targets, do not meet the organisational level required to disqualify the 'IT Army' as spontaneously assembled.[133] Therefore, 'IT Army' meets the criterion of spontaneity.

1.3.3. Inhabitants

Another salient criterion pertains to the eligibility of individuals to participate in a *levée en masse*. Article 4(A)(6) specifically designates 'inhabitants of unoccupied territory' as potential participants, though the definition of 'inhabitant' remains open to interpretation. Commonly, inhabitants are considered to be individuals who reside in a place on a regular or habitual basis, which introduces complexities regarding the involvement of foreigners in the defence of Ukraine.[134] Consequently, both Ukrainian and non-Ukrainian nationals who reside permanently in the territory under invasion and choose to resist are eligible to partake in a *levée en masse*.[135] Conversely, individuals, whether Ukrainian or non-Ukrainian, who are residents of other states do not meet this criterion and are thus excluded from participation.[136]

1.3.4. Geographical Scope

Article 4(A)(6) further stipulates that for inhabitants to qualify as a *levée en masse*, they must reside in unoccupied territories of the invaded nation. At the time of writing, reports suggest that Russian forces are occupying specific Ukrainian regions such as parts of Kherson and Zaporizhia oblasts.[137] Consequently, individuals residing in these occupied territories would be ineligible to be considered part of a *levée en masse* due to the presence of occupying forces. Nevertheless, the bulk of Ukrainian territory remains free from occupation. Therefore, those 'IT Army' volunteers residing in these unoccupied regions who engage in resistance activities against the invasion are potentially able to be recognised as a *levée en masse*.

The traditional rationale behind a *levée en masse* historically focuses on halting the progress of an invading army by confrontation on the frontline. However, the scope of what constitutes a *levée en masse* is not necessarily limited to physical confrontations directly against invading troops. In the context of modern warfare, especially with cyber operations, actions taken by civilians could extend to targeting military objectives located

[133] ibid.
[134] Wallace and Reeves (n 128); Buchan and Tsagourias (n 10).
[135] Wallace and Reeves (n 128); Buchan and Tsagourias (n 10).
[136] Buchan and Tsagourias (n 10).
[137] George Barros and others, 'Interactive Map: Russia's Invasion of Ukraine' <https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375> accessed 9 November 2025.

well beyond the immediate battle lines.[138] GCIII precludes the possibility that civilian-initiated operations targeting remote military objectives might qualify as a *levée en masse*. The principle of military necessity provides no substantial legal grounds to limit defensive cyber measures exclusively to engagements with on-the-ground invading forces.[139] Thus, cyber operations carried out by groups such as the 'IT Army' on targets such as mainland Russia could indeed be justified under the concept of *levée en masse*, suggesting that such operations, even when extending beyond traditional front lines, are permissible.

1.3.5. Carrying Arms Openly

As already discussed under subsection 1.2.4, the notion of 'carrying arms openly' in the context of cyber warfare is highly contentious. Although the concept of a cyber *levée en masse* is acknowledged,[140] employing devices such as laptops or other forms of cyber infrastructure does not adequately identify an individual as a combatant.[141] This distinction becomes crucial in the characterisation of a *levée en masse*, where visibly bearing arms is the sole criterion that differentiates participants from the civilian population. It is therefore suggested that within the framework of a *levée en masse*, the term 'openly' should be interpreted as 'visibly'.[142] Without a visible weapon, it proves challenging to distinguish participants of a theoretical cyber *levée en masse* from non-combatants.[143]

It is a complex issue to determine how the criterion of openly carrying arms can be applied to cyber weapons. While typical tools of cyber operations, such as laptops, can indeed be carried visibly, malware, which is also a form of cyber weapon, cannot.[144] Even in the case of visible possession, would that sufficiently distinguish combatants in a *levée en masse* from civilians, given that these devices are commonly used by non-combatants as well? These inherent difficulties have led some scholars to contend that the cyber *levée en masse* concept is 'simply an unworkable notion'.[145] This argument indeed has merit, particularly given the current requirements, unless they are interpreted in light of the unique characteristics of cyber warfare.

1.3.6. Adherence to IHL

The considerations under subsection 1.2.5 are equally relevant when discussing the concept of *levée en masse*, which shares similar requirements for adherence to IHL. In light of the previous analysis concerning the definition of cyber 'attack', it becomes evident that the classification of 'IT Army' activities under IHL is contingent upon the

[138] Waters (n 79) 782; Buchan and Tsagourias (n 10).
[139] Waters (n 79) 782.
[140] *Tallinn Manual* (n 51) r 88.
[141] Wallace and Reeves (n 128).
[142] Buchan and Tsagourias (n 10).
[143] Wallace and Reeves (n 78) 659.
[144] Buchan and Tsagourias (n 10).
[145] Wallace and Reeves (n 78) 660.

interpretative approach adopted. As discussed, the ICRC's broader interpretation of an 'attack' could suggest non-compliance by the 'IT Army' with IHL.[146] However, as explored, some scholars disagree with this approach and state practices also often adopt a narrower definition, focusing more on physical damage and direct military effects, suggesting a different evaluation.[147] Under these more restrictive criteria, the 'IT Army's' cyber operations, which generally do not pass the threshold of causing 'inconvenience', might not be classified as attacks, thereby aligning them more closely with the requirements of IHL.

Nonetheless, it should be concluded that the 'IT Army' does not fulfil the criteria for a *levée en masse*. Primarily, this is because the group, which operates via the Internet, ostensibly lacks a structured, hierarchical command necessary to enforce an internal disciplinary system. Additionally, the 'IT Army' does not satisfy the requirement of distinguishing themselves from civilians, as they fail to carry arms openly, a critical distinguishing feature in this context. Unlike irregular armed forces, which are required to also have a fixed distinctive sign, the open carrying of arms is the sole clear marker for a *levée en masse*. Consequently, it could appear more feasible for the 'IT Army' to meet the criteria for combatant status as a volunteer corps rather than as a *levée en masse*.[148]

As the analysis reveals, the 'IT Army' volunteers currently do not qualify as combatants. Consequently, they are classified as civilians, who are granted protection against attacks under IHL, 'unless and for such time as they take a direct part in hostilities'.[149] The critical question, therefore, is whether their activities amount to direct participation in hostilities or whether the 'IT Army' as a whole could be regarded as an Organised Armed Group. The context and criteria for DPH – threshold of harm, direct causation, and belligerent nexus – have been analysed in detail in the first part of this two-part study in relation to mobile app users. The following section builds on that foundation to assess their applicability to 'IT Army' volunteers.

1.4. 'IT Army' – An Organised Armed Group?

Before delving into the question of whether the operations of 'IT Army' volunteers align with the DPH criteria, it is crucial to address a pertinent distinction. The differentiation between civilians acting individually, sporadically, spontaneously, or within an unorganised framework and OAG members is fundamental, as the status of the latter is assessed differently under the rules on targeting. Two perspectives are important to mention in this regard. According to a more stringent approach, within an OAG, only

[146] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95) 41–42; See also Geiss and Lahmann (n 100); Kilovaty (n 110); Droege (n 99) 559.
[147] Schmitt, 'Cyber Operations and the Jus in Bello' (n 97) 95; Schmitt, 'France Speaks Out on IHL and Cyber Operations' (n 120); Droege (n 99) 559–560; Melzer, 'Cyberwarfare and International Law' (n 22) 26.
[148] Wallace and Reeves (n 78) 661–662.
[149] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 96) art 51(3).

members whose continuous function is to take a direct part in hostilities (continuous combat function) are legitimate targets regardless of their direct participation at any given moment.[150] In contrast, a broader view holds that mere membership in an OAG suffices to render individuals targetable.[151] Therefore, before examining the extent to which the 'IT Army' volunteers' activities may constitute DPH, it is essential to ascertain whether the 'IT Army' qualifies as an organised armed group.

The concept of an organised cyber armed group, as suggested by the Tallinn Manual, hinges on the presence of an established command structure capable of sustaining military operations.[152] While such organisations need not mirror the disciplined nature of conventional military units, the activities of small hacker groups typically do not fulfil this organisational criterion.[153] The Tallinn Manual refrains from defining precisely what constitutes a 'small group', instead advocating that organisational status be assessed on a case-by-case basis.[154] In any event, to be recognised as such, a group must demonstrate a level of organisation and be armed.

The Tallinn manual clarifies that the occurrence of numerous hackers attacking a state does not, in itself, constitute an organisation, even if their actions are cooperative.[155] A more challenging scenario arises with informal groupings of individuals who, while acting collectively – simultaneously yet without coordination – do not form an organised structure.[156] This scenario, which more closely resembles the situation of the 'IT Army', involves individuals accessing shared resources such as websites with hacking tools and target information, but without coordinating their attacks.[157] The consensus is that such informally aligned individuals do not meet the criteria to be considered an organised armed group.[158] Given this perspective, coupled with previously discussed sections indicating the 'IT Army's' lack of a command structure, it is clear that the 'IT Army' does not qualify as an organised group under the current framework.

Even if the 'IT Army' were to evolve into an organised structure, it would also need to be considered 'armed' to qualify as an organised armed group under the criteria relevant to cyber warfare contexts. In these scenarios, a group is deemed armed if it possesses the capability to conduct cyber-attacks.[159] Thus, the classification of the 'IT Army' as armed within IHL depends crucially on how the term 'attack' is interpreted vis-à-vis their

---

[150] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 70.
[151] The U.S. Department of Defense's Office of the General Counsel, *Law of War Manual* (2015) para 5.8.2.1; *Tallinn Manual* (n 51) r 96 para 4; Schmitt, 'The Law of Cyber Targeting' (n 3) 11.
[152] *Tallinn Manual* (n 51) r 83 para 11.
[153] ibid.
[154] ibid.
[155] ibid paras 13–14.
[156] ibid para 15.
[157] ibid.
[158] ibid.
[159] ibid para 11.

actions.[160] Although the definition of an 'attack' in cyber warfare remains contentious, as discussed under subsubsection 1.2.5.1, the implications of this term suggest that the 'IT Army' could be considered armed, as the criterion focuses on the *capacity* to undertake cyber-attacks. Employing a broader definition of 'attack',[161] the 'IT Army' indeed qualifies as 'armed' given their technical capabilities. Even adopting a more restrictive definition,[162] it remains difficult to conceive that a group of specialised individuals engaged in cyber support for a state within an armed conflict would lack the capability to execute cyber operations that could disrupt significant functionalities.

The analysis reveals that the 'IT Army' currently does not meet the criteria to be classified as an organised armed group, primarily due to its lack of formal organisation. Consequently, it is considered a collection of civilians. Therefore, only individuals whose actions constitute direct participation in hostilities may be targeted. The next step of this analysis will focus on determining whether the activities of the 'IT Army' volunteers qualify as DPH, which is crucial for establishing their targetability under IHL.

1.5. 'IT Army' – Civilians Directly Participating in Hostilities?

The first part of this two-part study analysed the context and criteria for direct participation in hostilities – threshold of harm, direct causation, and belligerent nexus – in relation to Ukraine's mobile app users. Building on that foundation, this section evaluates their applicability to 'IT Army' volunteers.

In assessing whether the 'IT Army' volunteers are directly participating in hostilities, a critical first step is to determine if their actions surpass the threshold of harm.[163] This threshold is not limited to actions resulting in physical damage but also includes activities that negatively impact the military operations or capacity of a party involved in the conflict.[164] Consequently, even cyber operations that do not amount to a cyber-attack could potentially cross this threshold if they significantly impair military functionality.

Based on the current reports, the cyber operations conducted by the 'IT Army', such as DDoS attacks targeting the Moscow Stock Exchange,[165] banks,[166] Russian government

[160] Schmitt, 'Cyber Operations and the Jus in Bello' (n 97) 100.
[161] ICRC, 'IHL and Challenges of Contemporary Armed Conflicts' (n 95); Geiss and Lahmann (n 100); Kilovaty (n 110); Droege (n 99).
[162] Schmitt, 'Cyber Operations and the Jus in Bello' (n 97); Schmitt, 'France Speaks Out on IHL and Cyber Operations' (n 120); Droege (n 99); Melzer, 'Cyberwarfare and International Law' (n 22).
[163] *ICRC Interpretive Guidance on DPH* (n 150) 46; *Tallinn Manual* (n 51) r 97 para 5.
[164] *ICRC Interpretive Guidance on DPH* (n 150) 47.
[165] Brewster (n 14).
[166] IT Army of Ukraine, '"Promsvyazbank, Alfa-Bank, Sberbank, the Electronic Passport System (EPTS), and Rosreestr Were Taken Down by Our Precise Attack" (Telegram Post)' (n 16); Brewster (n 14); Antoniuk (n 14).

websites,[167] food delivery services,[168] or other companies,[169] cannot meet this criterion. These operations, while disruptive, neither cause physical damage nor significantly impact Russian *military* capabilities. Cyber operations that involve gathering intelligence on Russia, or disrupting its communication networks and the coordination of its military personnel and equipment, or acts of cyber sabotage, could potentially meet the threshold of harm as they go beyond mere disruption and have a direct impact on military capabilities.[170] Yet, the operations reported so far fall short of crossing the threshold of harm necessary to be considered DPH under IHL.

The absence of the requisite threshold of harm essentially precludes the operations of the 'IT Army' volunteers to date from being classified as direct participation in hostilities. While it is conceivable that reported DDoS attacks might affect Russia's military capabilities, aligning with the characteristics of the direct causation criterion remains challenging.[171] These cyber operations, primarily targeted at, for instance, inflicting economic damage to diminish Russia's military capabilities,[172] would exemplify causing harm indirectly. While it remains conceivable that some activities of the 'IT Army' might meet the criteria for both the threshold of harm and direct causation,[173] the specifics of the reported cyber operations do not currently support such a scenario. If these two criteria are met, establishing a belligerent nexus might be relatively straightforward, given that the 'IT Army' explicitly positions itself as resisting the Russian invasion and supporting Ukraine's defence.[174] However, based on the available information, it can be concluded that the activities of 'IT Army' volunteers do not amount to direct participation in hostilities and therefore the volunteers retain their protected status as civilians under IHL.

Conclusion

The analysis in this study indicates that 'IT Army' volunteers do not qualify for combatant status under IHL, as they fail to meet the necessary conditions. Specifically, 'IT Army' volunteers do not qualify for combatant status under Article 4(A)(1) of the GCIII as members of regular armed forces because they are not formally integrated into Ukraine's armed forces. Furthermore, they do not meet the criteria under Article 4(A)(2) of the GCIII as members of irregular armed forces due to the absence of a clear and organised

[167] Ministry of Digital Transformation of Ukraine (n 17).
[168] IT Army of Ukraine, '"Yesterday, for Some Mysterious Reason, Customers of Food Delivery Services Were Unable to Use Them" (Telegram Post)' (n 18); Fendorf (n 18).
[169] IT Army of Ukraine, '"We Have Never Reached Such Heights Before" (Telegram Post))' (n 14).
[170] Buchan and Tsagourias (n 10).
[171] *ICRC Interpretive Guidance on DPH* (n 150) 46.
[172] Shaun Waterman, 'Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts' (*Newsweek*, 21 February 2023) <www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970> accessed 12 June 2024.
[173] See William Casey Biggerstaff, 'The Status of Ukraine's "IT Army" Under the Law of Armed Conflict' (*Lieber Institute*, 10 May 2023) <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/> accessed 7 June 2024; Biggio (n 65) 170–171.
[174] 'The Official Website of the IT ARMY of Ukraine' (n 9).

command structure, which is an essential requirement. Additionally, the 'IT Army' does not satisfy the stringent conditions set forth by IHL, as they do not wear a distinctive sign, do not carry arms openly, and do not adhere to the rules and customs of war. Consequently, they also do not fulfil the criteria for a *levée en masse* under Article 4(A)(6) of the GCIII.

Moreover, the analysis showed that although the 'IT Army' possesses the capability to conduct cyber-attacks and can be considered 'armed', they are not organised. Instead, they consist of a loosely aligned group of individuals and therefore do not qualify as an organised armed group. Additionally, the cyber operations conducted by the 'IT Army', such as distributed denial of service attacks, while disruptive, generally do not meet the threshold of harm required to classify them as directly participating in hostilities since they neither cause physical damage nor significantly impact Russian military capabilities. Consequently, 'IT Army' volunteers are civilians and retain their protected status under IHL.

IHL has often been criticised for being 'one war behind reality',[175] and the ongoing Russia-Ukraine armed conflict exemplifies this point. As this conflict demonstrates, technology has become an integral aspect of modern warfare. The increasing 'civilianization' and 'digitalization' of warfare blur the lines between combatants and civilians. This ambiguity presents significant operational challenges, particularly in determining whether an individual is targetable, which directly implicates the 'cardinal' principle of distinction.

The challenges identified in analysing the legal status of 'IT Army' volunteers highlight the difficulty in applying traditional legal constructs, designed for conventional warfare, to cyber warfare. Traditional combatant criteria, such as distinctive identification and openly carrying arms, are less applicable in cyber contexts, yet no definitive decisions have been made to address these nuances, leaving interpretations open-ended. Similarly, the definition of an 'attack', crucial for assessing adherence to IHL rules regarding combatant status, remains particularly controversial. As the criteria for wearing a distinctive sign and carrying arms openly, defining 'attack' is subject to varied interpretations. Adopting the broader definition suggested by the ICRC, which would include under the principle of distinction all forms of denial-of-service attacks, even those causing mere inconvenience, remains impractical due to a lack of support from state practice.

Given these challenges, the focus should shift from the creation of new laws (which face significant political and practical hurdles) to the cultivation of state practice and consensus on interpreting existing IHL norms in cyber contexts. Standardising definitions would enhance predictability and legal clarity. As states document consistent practices

[175] Marco Sassòli, Antonine A Bouvier and Anne Quintin, 'Historical Development of International Humanitarian Law', *How Does Law Protect in War?: Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, vol I (3rd edn, ICRC 2011) 3.

and integrate these into military and legal frameworks, customary international law may emerge, gradually filling the current normative gaps.

Judicial engagement could also play a decisive role. While in 2008 the world first witnessed the use of cyber operations within an international armed conflict between Russia and Georgia, the application of IHL to cyber warfare has yet to be addressed by international courts. Cases arising from the Russia-Ukraine armed conflict could provide authoritative guidance, clarifying the applicability of IHL to cyber operations and informing both state practice and doctrinal interpretation.

Ultimately, the evolving nature of modern warfare, marked by civilian participation, digitalisation, and decentralised operations, demands a flexible yet coherent legal approach. While 'IT Army' volunteers remain protected as civilians under current law, the ongoing development of cyber operations presents an urgent opportunity for states, scholars, and international institutions to ensure that IHL remains effective in protecting civilians while accommodating the realities of 21st-century conflict.

Bibliography

Antoniuk D, 'Ukrainian Hacktivists Claim to Leak Trove of Documents from Russia's Central Bank' (*The Record from Recorded Future News*, 7 November 2022) <https://therecord.media/ukrainian-hacktivists-claim-to-leak-trove-of-documents-from-russias-central-bank> accessed 30 May 2024

——, 'How Ukraine's Volunteer Hackers Have Created a "Coordinated Machine" Around Low-Level Attacks' (*The Record from Recorded Future News*, 4 April 2024) <https://therecord.media/ukraine-volunteer-it-army-machine-low-level-attacks> accessed 28 May 2024

Bannelier K, 'Is the Principle of Distinction Still Relevent in Cyberwarfare?' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015)

Barros G and others, 'Interactive Map: Russia's Invasion of Ukraine' <https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375> accessed 9 November 2025

Biggerstaff WC, 'The Status of Ukraine's "IT Army" Under the Law of Armed Conflict' (*Lieber Institute*, 10 May 2023) <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/> accessed 7 June 2024

Biggio G, 'The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict' [2024] Journal of International Humanitarian Legal Studies 1

Brewster T, 'Moscow Exchange, Sberbank Websites Knocked Offline - Was Ukraine's Cyber Army Responsible?' (*Forbes*, 28 February 2022) <www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/> accessed 30 May 2024

Buchan R and Tsagourias N, 'Ukrainian "IT Army": A Cyber Levée En Masse or Civilians Directly Participating in Hostilities?' (*EJIL: Talk!*, 9 March 2022) <www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/> accessed 6 January 2024

Burgess M, 'Russia Is Being Hacked at an Unprecedented Scale' (*Wired*, 27 April 2022) <www.wired.com/story/russia-hacked-attacks/> accessed 12 June 2024

Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022)

Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533

Feldstein S, 'Disentangling the Digital Battlefield: How the Internet Has Changed War' (*War on the Rocks*, 7 December 2022) <https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/> accessed 12 April 2024

Fendorf K, 'The Dynamics of the Ukrainian IT Army's Campaign in Russia' (*Lawfare*, 15 June 2023) <www.lawfaremedia.org/article/the-dynamics-of-the-ukrainian-it-army-s-campaign-in-russia> accessed 4 June 2024

Ford M, 'The Smartphone as Weapon Part 1: The New Ecology of War in Ukraine' (2022) <www.academia.edu/75845985/The_Smartphone_as_Weapon_part_1_the_new_ecology_of_war_in_Ukraine> accessed 30 April 2024

Geiss R and Lahmann H, 'Protecting Societies: Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (The Geneva Academy of International Humanitarian Law and Human Rights 2021) <www.adh-geneve.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf> accessed 5 June 2024

Gisel L and Olejnik L, 'The Potential Human Cost of Cyber Operations' (2019) ICRC Expert Meeting

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102 International Review of the Red Cross 287

Harrison Dinniss H, *Cyberwarfare and the Laws of War* (1st edn, Cambridge University Press 2012)

Healey J and Grinberg O, '"Patriotic Hacking" Is No Exception' (*Lawfare*, 27 September 2022) <www.lawfaremedia.org/article/patriotic-hacking-no-exception> accessed 5 June 2024

Hollis D, 'Cyberwar Case Study: Georgia 2008' [2011] *Small Wars Journal* <https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf> accessed 25 May 2024

ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (2015) 32IC/15/11 <www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf> accessed 7 June 2024

——, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper' (ICRC 2019) <www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf> accessed 5 June 2024

——, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2020) 102 International Review of the Red Cross 481

——, *Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War* (1st edn, Cambridge University Press 2021)

——, 'When Does International Humanitarian Law Apply to the Use of Information and Communications Technologies?' (2023) <www.icrc.org/sites/default/files/wysiwyg/war-and-law/01_when_does_ihl_apply-0.pdf> accessed 18 July 2024

'International Cyber Law in Practice: Interactive Toolkit' (*Cyber Law Toolkit*, 27 May 2024) <https://cyberlaw.ccdcoe.org/wiki/Main_Page> accessed 28 May 2024

Ipsen K, 'Combatants and Non-Combatants' in Dieter Fleck and Michael Bothe (eds), *The handbook of international humanitarian law* (Fourth edition, Oxford University Press 2021)

IT Army of Ukraine, '"Yesterday, for Some Mysterious Reason, Customers of Food Delivery Services Were Unable to Use Them" (Telegram Post)' (*Telegram*, 1 May 2022) <https://t.me/itarmyofukraine2022/320> accessed 6 April 2024

——, 'We Launched a DDoS Attack on Channels Showing Putin's Address to the Federal Assembly: 1TV, VGTRK and SMOTRIM (Telegram Post)' (*Telegram*, 21 February 2023) <https://t.me/itarmyofukraine2022/1054> accessed 7 June 2024

——, '"A Big Thank You to the Ministry of Digital Transformation @FedorovMykhailo for Recognizing Our Relentless Efforts and Recent Successes."' (*X (formerly Twitter)*, 11 October 2023) <https://x.com/ITArmyUKR/status/1712107660454105172?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1712107660454105172%7Ctwgr%5Eee68da5a84a5ff9accf1b3c1a26fe67c77ab40f7%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Ftherecord.media%2Fukraine-volunteer-it-army-machine-low-level-attacks> accessed 2 June 2024

——, '"Behold a Masterful Operation Prepared for Nearly a Month" (Telegram Post)' (*Telegram*, 13 March 2024) <https://t.me/itarmyofukraine2022/2041> accessed 29 May 2024

——, '"This Time We Have a Whole Set of Non-Working Internet Providers: Megafon, Chebnet, Wifire, Netbynet" (Telegram Post)' (*Telegram*, 19 March 2024) <https://t.me/itarmyofukraine2022/2067> accessed 29 May 2024

——, '"We Have Never Reached Such Heights Before" (Telegram Post))' (*Telegram*, 25 March 2024) <https://t.me/itarmyofukraine2022/2085> accessed 29 May 2024

——, '"Promsvyazbank, Alfa-Bank, Sberbank, the Electronic Passport System (EPTS), and Rosreestr Were Taken Down by Our Precise Attack" (Telegram Post)' (*Telegram*, 22 May 2024) <https://t.me/itarmyofukraine2022/2191> accessed 2 June 2024

James L, 'Military Information Sharing by Ukrainian Citizens in the Digital Environment: DPH? – Blurring of Lines Between Civilian and Military Actors in Ukraine' (*Opinio Juris*, 12 September 2022) <https://opiniojuris.org/2022/09/12/military-information-sharing-by-ukrainian-citizens-in-the-digital-environment-dph-blurring-of-lines-between-civilian-and-military-actors-in-ukraine/> accessed 12 April 2024

Kaska K, Osula A-M and Stinissen J, 'The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis' <https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/> accessed 29 May 2024

Kilovaty I, 'Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law' (2016) 23 Michigan Telecommunications & Technology Law Review 113

——, 'ICRC, NATO and the U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law' (2016) 15 Duke Law & Technology Review 1

Kirichenko D, 'How Ukraine Built a Volunteer IT Army from Scratch' (*Euromaidan Press*, 15 January 2024) <https://euromaidanpress.com/2024/01/16/how-ukraine-built-a-volunteer-hacker-army-from-scratch/> accessed 30 May 2024

McGuinness D, 'How a Cyber Attack Transformed Estonia' (*BBC*, 27 April 2017) <www.bbc.com/news/39655415> accessed 27 July 2024

Melzer N, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009)

——, 'Cyberwarfare and International Law' (United Nations Institute for Disarmament Research 2011) <https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 5 June 2024

——, 'The Principle of Distinction Between Civilians and Combatants' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (1st edn, Oxford University Press 2014)

Militarnyi, 'Президент підписав закон про електронний кабінет військовозобов'язаного [President Signed the Law on the Electronic Cabinet of Persons Liable for Military Service]' (*Мілітарний*, 2 April 2024) <https://mil.in.ua/uk/news/prezydent-pidpysav-zakon-pro-elektronnyj-kabinet-vijskovozobov-yazanogo/> accessed 29 May 2024

Ministry of Digital Transformation, 'Підсумки Роботи IT-Армії. Як Українські IT-Волонтери Забезпечували Кіберфронт [Results of the Work of the IT Army. How Ukrainian IT Volunteers Provided the Cyber Front] (Telegram Post)' (*Telegram*, 20 February 2023) <https://t.me/mintsyfra/3834> accessed 2 June 2024

Ministry of Digital Transformation of Ukraine, 'Ministry of Digital Transformation: IT Army Blocks Russian Sites in a Few Minutes - the Main Victories of Ukraine on the Cyber Front' (*Government Portal*, 28 February 2022) <www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti> accessed 16 June 2024

National Security and Defense Council of Ukraine, 'О. Данілов провів нараду з питань створення кібервійськ [O. Danilov Held a Meeting on the Creation of Cyber Forces]' (*Рада національної безпеки і оборони України*, 13 September 2021) <www.rnbo.gov.ua/ua/Diialnist/4995.html> accessed 29 May 2024

'Official Telegram Chanel of the It Army of Ukraine' (*Telegram*) <https://t.me/s/itarmyofukraine2022> accessed 9 November 2025

Pearson J, 'Ukraine's "IT Army" Targets Belarus Railway Network, Russian GPS' (*Reuters*, 3 March 2022) <www.reuters.com/world/europe/ukraines-it-army-targets-belarus-railway-network-russian-gps-2022-03-03/> accessed 4 June 2024

Render-Katolik A, 'The IT Army of Ukraine' <www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine> accessed 7 January 2024

Rodenhäuser T and Vignati M, '8 Rules for "Civilian Hackers" During War, and 4 Obligations for States to Restrain Them' (*Humanitarian Law & Policy*, 4 October 2023)

<https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/> accessed 4 June 2024

Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014)

Sassòli M, Bouvier AA and Quintin A, 'Historical Development of International Humanitarian Law', *How Does Law Protect in War?: Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, vol I (3rd edn, ICRC 2011)

Schmitt MN, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 Naval War College International Law Studies 89

——, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict. Proceedings 2012* (NATO CCD COE Publications, 2012 2012)

—— (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017)

——, 'The Law of Cyber Targeting' (2018) 68 Naval War College Review

——, 'France Speaks Out on IHL and Cyber Operations: Part II' (*EJIL: Talk!*, 1 October 2019) <www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/> accessed 7 June 2024

Shore J, 'Don't Underestimate Ukraine's Volunteer Hackers' (*Foreign Policy*, 12 January 2024) <https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/> accessed 7 January 2024

Soesanto S, 'The IT Army of Ukraine: Structure, Tasking, and Ecosystem' (Center for Security Studies (CSS), ETH Zürich 2022)

——, 'Ukraine's IT Army' (2023) 65 Survival 93

——, 'Ukraine's Counter-Hybrid Campaigns in Cyberspace' (The Hague Centre for Strategic Studies 2023)

The Associated Press, 'Ukraine Cyber Official: We Only Attack Military Targets' (*The Independent*, 4 March 2022) <www.independent.co.uk/news/ukraine-russia-kremlin-boston-hackers-b2028853.html> accessed 4 June 2024

'The Official Website of Team Onefist' (*Team Onefist*) <www.onefist.org> accessed 30 May 2024

'The Official Website of the IT ARMY of Ukraine' (*IT Army of Ukraine*) <https://itarmy.com.ua/?lang=en> accessed 21 May 2024

The U.S. Department of Defense's Office of the General Counsel, *Law of War Manual* (2015)

Tidy J, 'Ukraine Cyber-Conflict: Hacking Gangs Vow to De-Escalate' (*BBC*, 6 October 2023) <www.bbc.com/news/technology-67029296> accessed 4 June 2024

——, ‘Ukraine Gives Award to Foreign Vigilantes for Hacks on Russia’ (*BBC*, 3 April 2024) <www.bbc.com/news/technology-68722542> accessed 30 May 2024

Tikk E, Kaska K and Vihul L, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence (CCD COE) 2010) <https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/> accessed 13 June 2024

Turns D, ‘Cyber Warfare and the Notion of Direct Participation in Hostilities’ (2012) 17 Journal of Conflict and Security Law 279

Wallace D and Reeves S, ‘The Law of Armed Conflict’s “Wicked” Problem: Levee En Masse in Cyber Warfare’ (2013) 89 International Law Studies 646

——, ‘Levée En Masse in Ukraine: Applications, Implications, and Open Questions’ (*Lieber Institute*, 11 March 2022) <https://lieber.westpoint.edu/levee-en-masse-ukraine-applications-implications-open-questions/> accessed 9 June 2024

Waterman S, ‘Ukraine’s Volunteer Cyber Army Could Be Blueprint for the World: Experts’ (*Newsweek*, 21 February 2023) <www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970> accessed 12 June 2024

——, ‘Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army’ (*Newsweek*, 14 March 2023) <www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814> accessed 15 May 2024

Waters C, ‘New Hacktivists and the Old Concept of Levée En Masse’ (2014) 37 The Dalhousie Law Journal 771

Watts S, ‘Combatant Status and Computer Network Attack’ (2010) 50 Virginia Journal of International Law 391

——, ‘The Notion of Combatancy in Cyber Warfare’ in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict. Proceedings 2012* (NATO CCD COE Publications 2012)

‘We Are Creating an IT Army - Tweet by Mykhailo Fedorov’ (*X (formerly Twitter)*) <https://twitter.com/FedorovMykhailo/status/1497642156076511233> accessed 7 January 2024

Yelagina S, ‘Законопроєкт Про Кіберсили ЗСУ Вже Обговорюють у МО Та Силах Оборони. Ми Дізнались Більше Про Майбутній Рід Військ [The Draft Law on the Cyber Forces of the Armed Forces of Ukraine Is Already Being Discussed in the Ministry of Defense and the Defense Forces. We Learned More About the Future Branch of the Military]’ (*AIN.Capital*, 8 May 2024) <https://ain.ua/2024/05/08/cyberforce/> accessed 29 May 2024

Zetter K, ‘An Unprecedented Look at Stuxnet, the World’s First Digital Weapon’ (*Wired*, 3 November 2014) <www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 27 July 2024

‘Проект Закону Про Кіберсили Збройних Сил України [Draft Law on Cyber Forces of the Armed Forces of Ukraine]’ (*Verkhnova Rada of Ukraine*) <https://itd.rada.gov.ua/billInfo/Bills/Card/45453> accessed 9 November 2025

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion [1996] ICJ Reports (International Court of Justice)

Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict 1977

Convention (III) Relative to the Treatment of Prisoners of War 1949

University of Glasgow

LEUPHANA
UNIVERSITÄT LÜNEBURG

INSTITUT
BARCELONA
ESTUDIS
INTERNACIONALS

ULB UNIVERSITÉ
LIBRE
DE BRUXELLES

UNIVERSITY
OF TARTU
1632

Radboud Universiteit

Co-funded by
the European Union